# 目　录

一般认为，抽象代数是以伽罗瓦理论的产生作为分界线的．十九世纪二十年代以前，代数学还着重于研究求解代数方程，当然也要讨论多项式理论等等．法国青年数学家伽罗瓦（É. Galois，1811～1832）用群的观点来研究代数方程的解，解决了古代的一个难题：一般的高于四次的代数方程没有根式解．从此，还由于其他一些学科的需要，代数学的研究逐渐转向研究各种代数结构．二十世纪以来，数学得到了蓬勃发展，各个数学分支都会有些代数结构，代数学就渗透到许多数学分支中，几乎成了它们的基础．内容广泛、抽象，这是抽象代数学的一个特点，不大可能通俗地讲清楚；特别是，由于种种原因，在我国的大学数学专业中，代数课程的比例太小，学得太少．

代数结构中，最简单和常见的是群、环、域．

# 一、群　论

所谓群，是一个带着一个运算的集合 $G$，它对这个运算满足结合律；并且，具有单位元素 $e$；$G$ 中每个元素 $a$ 都有逆元素 $a^{-1}$．

如果 $G$ 中的元素的个数是有限的，就称 $G$ 为**有限群**；否则，就是**无限群**．

群的最普遍的作用，是表达事物的对称性．在许多学科中，经常运用群来分类．一个最根本的问题是：究竟有多少群（如果同构的群看作是一样的话）．也就是怎样对群加以分类．无限群的分

类是非常复杂的；把所有的有限群找出来也不简单．最简单的群是交换群，就是群 $G$ 满足：对 $a$、$b\in G$，总有 $ab=ba$．

## 1. 有限交换群

关于有限交换群的结构，有个基本定理：任一有限交换群 $G$，总是一些循环子群的直积

$$G\cong H_{11}\otimes H_{12}\otimes\cdots\otimes H_{1\alpha_1}\otimes H_{21}\otimes\cdots\otimes H_{2\alpha_2}\otimes\cdots\otimes H_{s1}\otimes\cdots\otimes H_{s\alpha_s},$$

其中 $H_{ij}$ 是阶为 $p_i^{a_{ij}}$ 的循环群，$p_1$、…、$p_s$ 为素数，$a_{ij}\geqslant 0$ 为整数，而且 $p_i^{a_{ij}}$ 由 $G$ 所唯一确定．

由这个基本定理，有限交换群的分类就完全清楚了：每个交换群确定一组不变量 $(p_1^{a_{11}}, p_1^{a_{12}}, \cdots, p_1^{a_{1\alpha_1}}; p_2^{a_{21}}, p_2^{a_{22}}, \cdots, p_2^{a_{2\alpha_2}}; \cdots; p_s^{a_{s1}}, \cdots, p_s^{a_{s\alpha_s}})$，可以用以分类有限交换群；同构的群有相同的不变量；具有不同不变量的群互不同构；任意这样的一个数组，都有一个有限交换群以它为不变量．这就叫做“有限交换群的完全不变量组”．讨论一个结构的分类，最理想的是能找出这结构的完全不变量组，但这并不很容易．

由这个基本定理，任一有限交换群 $G$ 的元素可以标准地表达出，它的元素间的运算都能写得出，它的子群、商群等等都非常清楚．这就叫“群 $G$ 的结构清楚了”．

这个定理稍加修改，就可扩充为有限生成的变换群的基本定理．这个定理很有用，譬如在拓扑学中，同调群的结构就由它表出．

怎样研究一般的有限群？常用的办法是研究它的子群和商群．

所谓群 $G$ 的**子群** $H$，是指：$H$ 是 $G$ 的子集；而且 $H$ 关于 $G$ 中的运算是封闭的；$H$ 中每个元素的逆元素仍在 $H$ 中．

对 $a\in G$，集合 $aH=\{ah|h\in H\}$ 称为 $H$ 的一个**左陪集**．同样，$Ha$ 称为 $H$ 的一个**右陪集**．如果右陪集都是左陪集（即对每个 $a\in$

$G, aH=Ha$),这样的子群 $H$ 特别重要,称为 $G$ 的**正规子群**(或说"$H$ 在 $G$ 中正规"). 如果 $H$ 是 $G$ 的正规子群, 那么左陪集(也是右陪集)的全体所成的集合 $G/H=\{eH, a_2H, \cdots, a_sH\}$ 中定义运算 $aH\cdot bH=abH$ 后构成一个群,称为 $G$ 的**商群**(关于 $H$). 如果群 $G$ 除了自己和只含 $e$ 一个元素的正规子群外, 没有其他正规子群, 这种群 $G$ 称为**单群**(简单的意思, 就是除了显然的以外, 它没有正规子群).

## 2. 若当-霍尔德定理

可以用单群来描述一般的群. 因为是有限群, 我们总可以对群 $G$ 做出一连串的子群 $G\supset G_1\supset G_2\supset\cdots\supset G_n=\{e\}$, 其中 $G_1$ 在 $G$ 中正规, $G_2$ 在 $G_1$ 中正规, ……, $G_{i+1}$ 在 $G_i$ 中正规, 称为 $G$ 的**正规列**. 而且, 总可以做到商群 $G/G_1$, $G_1/G_2$, $\cdots$, $G_{n-1}/G_n=G_{n-1}$ 都是单群(这是因为, 如果不是单群的话, 总可以再在中间插进一些子群,使得商群都是单群). 这时的正规列,就称为**合成列**,它的一系列商群称为 $G$ 的**合成因子**. 关于合成列,有一个重要定理,叫做若当-霍尔德(C. M. E. Jordan-O.Hölder)定理,这是上一个世纪的事:有限群 $G$ 的合成因子由 $G$ 所唯一确定, 即对于 $G$ 的任意两个合成列 $G=G_0\supset G_1\supset\cdots\supset G_n=\{e\}$ 及 $G=H_0\supset H_1\supset\cdots\supset H_m=\{e\}$,必成立 $m=n$,且有 $\{1, 2, \cdots, n\}$ 的一个置换 $\pi$ 使单群 $G_{i-1}/G_i\cong H_{\pi(i)-1}/H_{\pi(i)}$(这里 $i=1, 2, \cdots, n$). 也即除了次序之外, 合成因子一一同构.

这样一来, 可以把有限单群勉强看作一般有限群的基石. 根据若当-霍尔德定理,一般有限群的分类与结构可以归结为两个问题: 单群的分类与结构, 以及群的扩张问题. 所谓群的扩张问题, 是已知子群 $G_1$ 和商群 $G/G_1$ 的结构,如何作出群 $G$ 来. 这是很难的问题,直到现在,所知道的结果不太多.

哪些群是单群?是否能把全部有限单群找出来?通过一百多年

来许多许多代数学家的努力，总算在1981年把有限单群的分类全部解决了．大家知道，最简单的有限单群是素数阶的循环群(因为子群的阶总是群的阶的因子，而素数是没有非显然的因子的，素数阶的群连非显然的子群都没有，因此是单群)．除了这些显然的单群外，最早知道的单群是**交代群** $A_n$(其中 $n\geqslant5$)，就是所有 $n$ 个文字的偶置换所组成的群，这还是十九世纪二十年代伽罗瓦所证明的结果．

## 3. 伽罗瓦理论与群

早在一百五十年以前，伽罗瓦就用群的观点来探讨代数方程根式解的问题：对于每个代数方程

$$f(x)\equiv a_0x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n=0,$$

都可以引进一个包含它的所有根和基域 $\mathbf{Q}$ 的最小数域 $K$，然后考虑 $K$ 的所有使 $\mathbf{Q}$ 和 $f$ 的系数都不变的自同构，它成一群 $G$，就称为方程 $f(x)=0$ 的**伽罗瓦群**，它是一个有限群．伽罗瓦给出了这个代数方程有根式解的充要条件是它的伽罗瓦群是可解群(所谓**可解群**，是指它的合成因子都是素数阶的单群．"可解群"这个名称，也正是从伽罗瓦的这个判别准则得来的)．伽罗瓦还证明了交代群 $A_n$ 当 $n\geqslant5$ 时是单群，而一般 $n$ 次方程的伽罗瓦群是**对称群** $S_n$ (即全体 $n$ 阶置换所组成的群)．当 $n\geqslant5$ 时 $S_n$ 的合成因子是 $A_n$ 和一个二阶循环群，所以 $S_n$(当 $n\geqslant5$ 时)不是可解群，从而一般的 $n$ 次代数方程($n\geqslant5$)不能有根式解，这就彻底解决了古代留下的一个难题．不光这个难题，运用伽罗瓦理论还能解决三等分任意角、倍立方等其他一些古代难题．伽罗瓦理论的产生，促使了有限群理论的发展，也促使了域的理论的发展，因为从本质上讲，伽罗瓦理论给出了有限正规扩域 $K$ 的子域与使基域不变的 $K$ 的自同构群 $G$ 的子群之间的一一对应关系，所以伽罗瓦理论与"域论"有着密切关系．以研究代数数域为对象的"代数数论"，就以伽罗瓦理

论为它的基石之一. 古典的伽罗瓦理论是域上的伽罗瓦理论. 近代许多数学家正在研究体(除环)上的伽罗瓦理论以及环上的伽罗瓦理论,这些对于环的结构的了解都起着重要的作用,形成"环论"研究中的一个极重要的方向.

伽罗瓦的反问题,是一百多年来长期未解决,又是许多数学家感兴趣的问题. 问题的提法是这样的:对于一个给定的有限群 $G$,是否存在一个有理系数的代数方程,使得它关于有理数域 $\mathbf{Q}$ 的伽罗瓦群同构于 $G$? 一百多年来,虽经许多数学家的努力,还是没有彻底解决,可见问题极难. 对一些特殊情况,问题是容易解决的,譬如 $G$ 为对称群 $S_n$ 或交代群 $A_n$ 时,答案都是肯定的. 1954年,苏联数学家萨伐列维奇(И. Р. Шафаревич)证明了:当 $G$ 是有限可解群时,问题是肯定的. 近年来,著名代数学家,菲尔兹奖获得者汤普森(J. G. Thompson)及其合作者致力于这个问题. 1985年,在北京国际群论会议上,汤普森就他近年来的工作作了报告,他的结果大致是说:在一定条件下,伽罗瓦群的交换扩张*)是伽罗瓦的. 伽罗瓦问题的一般情况,还远没有解决.

## 4. 典型群、连续群与李群

群的理论的发生与发展,一方面是由于伽罗华理论促使研究有限群,另一方面,也是研究典型群的需要. 二十世纪初,德国大数学家克莱茵(F. Klein, 1849~1925)把几何和变换群联系起来,从而也就促使人们去研究这些群的结构、性质等. 这些群,现在把它们叫做**典型群**. 它们都可以用矩阵形式来表示,而矩阵的元素都在实数域 $\mathbf{R}$ 或复数域 $\mathbf{C}$ 中:

所有 $n$ 阶非异方阵的全体,按矩阵乘法构成的群,叫做 $n$ 阶**一般线性群**,记作 $GL_n(\mathbf{R})$ 或 $GL_n(\mathbf{C})$(按系数在 $\mathbf{R}$ 或 $\mathbf{C}$ 中而定).

所有行列式为 1 的 $n$ 阶方阵全体所成的群,叫做**特殊线性群**,

*) 若群 $G$ 有交换的正规子群 $H$,则称 $G$ 为 $G/H$ 交换扩张.

记作 $SL_n(\mathbf{R})$ 或 $SL_n(\mathbf{C})$（按系数在 $\mathbf{R}$ 中或 $\mathbf{C}$ 中而定）.

所有满足 $\sigma\cdot{}^t\sigma=I_n$[*]的 $n$ 阶方阵 $\sigma$ 的全体组成的群，称为**正交群**，记作 $O_n(\mathbf{C})$ 或 $O_n(\mathbf{R})$（按系数在 $\mathbf{C}$ 中或 $\mathbf{R}$ 中而定）.

所有满足 $\bar{\sigma}\cdot{}^t\sigma=I_n$ 的 $n$ 阶复数方阵 $\sigma$ 全体所组成的群，称为**酉群**，记作 $U(n)$.

令 $2n$ 阶方阵

$$A=\begin{pmatrix} 0 & 1 & & & & & \\ -1 & 0 & & & & 0 & \\ & & 0 & 1 & & & \\ & & -1 & 0 & & & \\ & & & & \ddots & & \\ & 0 & & & & 0 & 1 \\ & & & & & -1 & 0 \end{pmatrix}.$$

所有满足 ${}^t\sigma A\sigma=A$ 的 $2n$ 阶方阵 $\sigma$ 的全体所组成的群，称为**辛群**，记作 $\mathrm{sp}_n(\mathbf{C})$ 或 $\mathrm{sp}_n(\mathbf{R})$（按系数在 $\mathbf{C}$ 中或 $\mathbf{R}$ 中而定）.

与射影几何有关的，就要研究射影群. 在上述这些典型群中，关于中心子群[**]所得的商群，就是相应的**射影群**. 例如 $GL_n(\mathbf{C})$ 的中心是所有 $aI_n$（其中 $a\neq 0$ 是复数），记作 $\mathbf{C}^*I$，于是 $GL_n(\mathbf{C})/\mathbf{C}^*I$ 就称**一般射影线性群**，记作 $PGL_n(\mathbf{C})$. 类似地，有 $PSL_n(\mathbf{C})$、$PSL_n(\mathbf{R})$ 等. 我国数学家华罗庚、万哲先等对典型群的研究作出很大贡献，著有《典型群》一书.

从这些典型群的研究，引出代数学中两个极其重要的分支：一个是李群，一个是李型群.

一个群 $G$ 如果又是拓扑空间，而且群的运算和元素求逆在这个拓扑下是连续的，则称 $G$ 为**连续群**，或称**拓扑群**. 上述一些典型群都是连续群.

---

[*] ${}^t\sigma$ 是指 $\sigma$ 的转置矩阵，$\bar{\sigma}$ 表示 $\sigma$ 中每一系数取共轭所得的矩阵；$I_n$ 为 $n$ 阶单位方阵.

[**] 群 $G$ 中与每个元素都可交换的元素，称为中心元素. $G$ 的全体中心元素形成 $G$ 的正规子群，称为 $G$ 的**中心**，常以 $Z(G)$ 表示.

一个拓扑空间，如果每点有邻域与 $n$ 维欧氏空间 $R^n$ 同胚，那就称为**流形**. 这时，每点附近就可以设置局部坐标. 如果局部坐标间的变换是解析函数，则称这个坐标系为解析坐标系，这个空间就称为**解析流形**.

如果一个群 $G$，它既是解析流形，而且群的运算与求逆在解析坐标系下都可以用解析函数来表达，那么就把 $G$ 叫做**李群**. 这个名词是为了纪念挪威数学家李(M. S. Lie, 1842～1899)，是他第一个在上世纪末系统地研究了局部李群.

李群的结构，从群来说，它是代数的；从拓扑空间来说，它是几何的；从解析函数来说，它是分析的，因此，它的分类、结构、性质，与数学的各个方面都有联系，应用非常广泛，在理论物理中也占着重要地位，以致有人称它是"数学的核心".

紧致李群的分类，早就由外尔(C. H. H. Weyl, 1885～1955)所完成. 他把这个问题最终地归结为复单李代数的分类：复单李代数一共分四大类与五个特殊代数(记作 $A_n$, $B_n$, $C_n$, $D_n$ 及 $E_6$, $E_7$, $E_8$, $F_4$, $G_2$). 四大类的单李代数都是典型群的李代数. 如果说李群是代数、几何、分析的结合，那么，李代数则是纯代数的结构了.

李群中，一个非常基本的问题是：是否每一个局部是欧几里得空间的连续群都是李群. 这是著名的希尔伯特(D. Hilbert, 1862～1943)的第五问题. 通过半个世纪许多人的努力，终于在1952年由格利森(A. M. Gleason)、蒙哥马利(D. Montgomery)、齐宾(L. Zippin)共同完全肯定地解决了.

## 5. 李型单群

由典型群所引出的另一重要方向，是李型群. 前面我们说，典型群是系数在实数域或复数域中满足某些条件的矩阵所成的群. 其实，系数不一定是实数或复数，只要是在某一个域(也可以是有

限域)中，也可以成群．例如系数在有限域$F_p$(即$p$个元素的域，$p$为素数)中所有$n$阶非异方阵的全体构成一般线性群，记作$GL_n(F_p)$．同样，有特殊线性群$SL_n(F_p)$，辛群$sp_n(F_p)$，正交群$O_n(F_n)$，等等．这些都是有限群，称为**有限典型群**，其中许多都是单群．十九世纪时就已知道这些有限典型群中的单群，除了素数阶的循环群及$A_n$之外($n\geqslant5$)，还知道由马蒂厄(E. L. Mathieu)所发现的五个散在的单群(不属系列的个别单群)，称为**马蒂厄群．**本世纪初，迪克逊(L. E. Dickson)还根据$G_2$型李群的形象，做出$G_2$型的有限单群．后来，几乎半个世纪没有人能发现其他有限单群．1955年，舍瓦莱(C. Chevalley)运用复单李代数的分类、结构、性质，在任意域$F$上构作了一系列单群，现在称为**舍瓦莱群．**当$F$是有限域时，这些舍瓦莱群都是有限单群，它们不仅包含了已知的有限典型群中的单群，也包含了迪克逊$G_2$型单群，而且还新造出$E_6$、$E_7$、$E_8$、$F_4$型单群．舍瓦莱的功绩不光是找出了新的有限单群，还在于他统一地处理了过去都是个别处理的有限典型群．从他开始，有了一个统一的工具来讨论原先以为互不相关的一大堆单群．继舍瓦莱之后，斯坦堡(R. Steinberg)、苏楚基(M. Suzuki)、利(R. -H. Ree)等人把舍瓦莱群作了某些改进，又得到了一连串有限单群，这些群现在统称为**李型单群**．五十年代中期，对有限群理论来说是划时代的．一方面，有舍瓦莱群的产生；另一方面，布劳尔(R. D. Brauer)给出了有限单群的一个非常重要的性质，研究群中对合(阶为2的元素)的中心化子．遵循他的思路，1966年詹科(Z. Janko)第一个作出了五个马蒂厄群以外的第一个散在单群，从此，散在有限单群像雨后春笋般冒出来．通过许多人共同努力，特别是汤姆森(W. Thomson)、哥伦斯坦(D.Gorenstein)、阿什巴彻(M.Aschbacher)等，最终于1981年，大家认为有限单群的分类解决了：(1)素数阶的循环群；(2)交代群$A_n$，$n\geqslant5$；(3)李型单群；(4)26个散在单群．这样一个能够简捷地说明的结果，竟历时三十载(从五十年代算起)，通过几百名数学家写成的

300～500 篇论文才完成．直至现在，还没有人完整地把证明写出来，但是大家认为是解决了的．不过，大家也认为有必要努力去做简化工作．当前，简化工作中的一个重要工具，是蒂茨(J. Tits)系统与蒂茨几何，它几乎已经独立系统地成为群论中的一个分支．

## 6. 蒂茨系统与蒂茨几何

设群 $G$ 有两个子群 $B$ 与 $N$，满足

(i) $B\cup N$ 生成 $G$；

(ii) $B\cap N$ 在 $N$ 中正规，而且 $W=N/B\cap N$ 是由一组二阶元素集 $S$ 所生成的，设 $S=\{s_i\}$，$s_i$ 在 $N$ 中原像取为 $n_i$；

(iii) 对 $s_i\in W$，有 $n_iBn_i\neq B$；

(iv) $n_iBn\subseteq Bn_inB\cup BnB$，对每 $n\in N$．

于是，就称 $G$ 为一个**蒂茨系统**或称作 ***B*-*N* 对**，记作 $G=(G, B, N, S)$．这个定义看来很不自然，但是，如果了解了舍瓦莱群的结构与性质，就知道它是舍瓦莱群的推广，而且蒂茨证明了秩大于等于 3 的有限 $B$-$N$ 对单群一定是李型单群．对应于蒂茨系统，可以相应地作一个几何，就是**蒂茨几何**．人们企图作一些结构，使得能在更大范围内统一有限单群，看来这还是较难的．

## 7. 代　数　群

人们可以从另一角度来研究舍瓦莱群，那就是五十年代几乎与舍瓦莱群同时兴起的“代数群”．代数群是代数流形[*]与群结构的结合．一个群 $G$，如果它还是一个代数流形，而且群的运算与求逆都是代数流形意义下的态射，那么就称 $G$ 为**代数群**．典型群都是代数群．譬如 $SL_n(K)$（这里 $K$ 为数域）就是仿射空间$\{(x_{11}, x_{12}, \cdots, x_{nn})\mid x_{ij}\in K\}$中满足一个代数方程：$\det(x_{ij})=1$ 的点$(x_{ij})$的全

*) 满足有限个代数方程的点的全体所成的集合，叫做代数流形．

体；另一方面，它又是群，而且群的运算与求逆用坐标形式表达出来是多项式函数，所以它是代数群．由矩阵组成的代数群，叫**线性代数群**．研究得最多的也就是线性代数群．舍瓦莱群都是线性代数群．五十年代时舍瓦莱对代数闭域 $K$ 上的半单线性代数群作了完整的分类．代数群与李群有许多相似的地方，有一个本质的差别是：李群考虑的基域是实数域 $\mathbf{R}$ 与复数域 $\mathbf{C}$，而代数群的基域是任意的代数闭域 $K$，它可以特征数不是零，因而代数群上没有自然的拓扑（可以用代数性质给出不是豪斯多夫 (F. Hausdorff) 的查里斯基(O. Zariski)拓扑）．然而，对复连通半单李群，可以有唯一的一个线性代数的结构．在这意义上，半单线性代数群是半单李群的扩充．

半单线性代数群与李型有限群有着非常密切的关系．六十年代末，斯坦堡曾证明：任一李型群都是相应的半单线性代数群在弗罗贝尼乌斯(F.G. Frobenius)变换下不变元素所成的集合．所以，研究李型群要从代数群着手；特别是研究李型群的表示，常常从代数群的表示局限过来，而代数群的表示本身又是具有非常丰富内容的方向．

## 8. 变换群的不变量

变换群的不变量，是指在变换群 $G$ 作用下不变的元素．研究不变量的问题，几乎是所有数学中经常碰到的问题．德国数学家克莱茵就把几何看作是研究变换群下的不变量：欧几里得几何就是研究运动群下的不变量，仿射几何就是研究仿射变换群下的不变量，等等．这里，我们需要对群的“作用”给一个定义：设 $G$ 为群，$M$ 为一集合，若有从集合 $G\times M=\{(g, x) \mid g\in G, x\in M\}$ 到集合 $M$ 内的一个映射 $f$，它满足：

(i) $f(g_2, f(g_1, x))=f(g_1\cdot g_2, x)$，其中 $g_1$、$g_2\in G$，$x\in M$；

(ii) $f(e, x)=x$，其中 $e$ 为 $G$ 的单位元素，$x\in M$，

这样，就称"$G$ 作用在集合 $M$ 上"，$f$ 就是**作用**．对每一 $g\in G$，就决定了一个从 $M$ 到 $M$ 的映射 $f(g,\ -)$：$x\mapsto f(g,\ x)$，所以，作用也可以看作 $G$ 中元素用 $M$ 到 $M$ 的映射表示出来，所以也叫**表示**．如果每个 $f(g,\ -)$ 都是 $M$ 到自身的双射(即置换)，那就把这个作用叫做 $G$ 的**置换表示**．如果 $M$ 是域 $K$ 上的向量空间，而且每个 $f(g,\ -)$ 都是 $M$ 的 $K$-线性变换，那就叫做 $G$(在 $M$ 上)的**线性表示**．$G$ 的线性表示理论，是研究群的最主要工具．

群 $G$ 通过 $f$ 作用在集合 $M$ 上，所谓"不变量"是指满足

$$f(g,\ x)=x$$

(对所有 $g\in G$)的元素 $x$．经常要研究不变量所成的集合．最简单的例子是所有 $n$ 个文字的置换所成的对称群 $S_n$ 作用在 $n$ 个变量的多项式环 $K[x_1,\ \cdots,\ x_n]$ 上，作用方式是变量进行置换．例如

$$f\left(\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix},\ x_1^3+x_1x_3+x_2^2\right)=x_3^3+x_3x_2+x_1^2,$$

这时候的不变量，就是域 $K$ 上的对称多项式．高等代数的知识告诉我们，有一个叫做"对称多项式的基本定理"：有 $n$ 个初等对称多项式

$$\begin{aligned}\sigma_1&=x_1+x_2\cdots+x_n,\\ \sigma_2&=x_1x_2+x_1x_3+\cdots+x_{n-1}x_n,\\ &\cdots\cdots\cdots,\\ \sigma_n&=x_1x_2\cdots x_n,\end{aligned}$$

对称多项式的全体$=K[\sigma_1,\ \cdots,\ \sigma_n]$；而且，$\sigma_1,\ \cdots,\ \sigma_n$ 关于 $K$ 是代数无关的．这就是说，任一对称多项式总是初等对称多项式的多项式，而且，这些初等对称多项式之间没有任何代数关系(即这些初等对称多项式不满足任何 $n$ 个变量的非零代数方程)．长远以来(一百多年)人们要问对于其他的群(线性群或群的线性表示)，用上述方式作用在多项式环 $K[x_1,\ \cdots,\ x_n]$ 上是否也可以找到有限多个不变多项式，使得任一个不变多项式都是这些不变多项式的多项式．这是希尔伯特第十四问题，是多项式不变量的有限性

问题．早在 1868 年，哥尔当(P. Gordan)就证明了对 $G=SL_2(\mathbf{C})$ 的情形．希尔伯特在提出著名的二十三个问题之前就证明了对 $G=SL_n(\mathbf{C})$ 的情形．本世纪二十年代，外尔对复半单李群证明了希尔伯特第十四问题，诺特(A. E. Noether, 1882～1935)对有限群证明了这个问题．但是，1959 年日本数学家永田雅宜(M. Nagata)举出了一个反例，否定了这个问题．对一般线性群，有限性定理不成立．这就对希尔伯特第十四问题提出了有哪些线性群能使之成立的问题．五十年代代数群理论兴起之后，人们着重研究线性代数群的多项式不变量的有限性问题．1964 年永田雅宜又证明了简约代数群的情况．然而，对非简约代数群，情况如何还不清楚，当前还在发展，在对幺幂代数群进行研究．苏联数学家波波夫(M. B. Попов)与波谋宁(K.Pommerening)有一个著名的猜测，至今未解决．1987 年世界数学家大会上波波夫做了一个 45 分钟的综合报告，也说明这个方向不断在发展．

## 9．群的表示理论

这是研究群的最重要工具．“表示”是指线性表示，即群 $G$ 到群 $GL_n(K)$(其中 $K$ 为域，称为表示的基域)内的同态 $\rho$: $G\to GL_n(K)$．因为 $GL_n(K)$ 中元素都可看作 $n$ 维线性空间 $V$ 上的非异线性变换，所以表示的意思也就是 $G$ 用 $V$ 上的线性变换群表示出来；不过，这时候是同态，而不是同构．若把 $G$ 在 $V$ 上的作用定义为 $g\cdot v=\rho(g)(v)$(其中 $g\in G$, $v\in V$)，于是 $\rho(G)$ 就成为 $V$ 上的线性变换群，这时候的 $V$ 也就叫做“$G$-模”．群 $G$ 的表示与 $G$-模是一一对应的，可以把它们看作一回事．这是诺特研究表示论的观点．其实，$V$ 不一定限于有限维 $n$，$K$ 也不一定是域，都可以谈 $G$ 的表示问题．

有限群、代数群、李群都各有自己的表示理论．对代数群来讲，就要求同态 $\rho$ 是代数群同态．同样，对李群，$\rho$ 不光是抽象代

数结构的同态. 为简单起见,这里只讲有限群的表示.

表示的一个核心问题,是把所有的表示找出来. 群 $G$ 的最基本的表示,是 $G$ 的"不可约表示": 设 $V$ 为 $G$-模,若 $V$ 除了$\{0\}$与本身外没有其他 $G$-子模(即 $G$ 稳定的 $V$ 的子空间),则称 $V$ 为**不可约 $G$-模**(或表示). 有些情况下,不可约 $G$-模构成所有 $G$-模的基石. 那就是,$K$ 特征数为 0,或 $K$ 的特征数 $p$ 除不尽 $G$ 的阶数,这时候任一 $G$-模 $V$ 都是不可约 $G$-模的直和 $V=V_1\oplus\cdots\oplus V_r$,其中 $V_i$ 都是不可约 $G$-模. 这叫做 $V$ 是**完全可约的**. 有限群表示具有完全可约性. 这种情况下讨论群 $G$ 的表示理论,就叫做**常表示理论**;否则,是**模表示理论**. 两者的最大区别是: 在常表示理论中, 不可约 $G$-模与不可分解 $G$-模(不能分解成两个非显然 $G$-子模的直和的 $G$-模)是一致的;在模表示论中就不一致,两者关系很复杂, 也就成为模表示理论中主要问题之一. 下面主要谈常表示的性质.

$G$ 给定之后, 有多少个不可约 $G$-模? 这些不可约模的维数是多少? 常表示理论中的一个基本定理是: 不可约模个数(同构看作一样)等于 $G$ 的共轭类个数 $h$. 设 $V_1$, $V_2$, $\cdots$, $V_h$ 为不可约模全体, $d_i=\dim_K V_i$ 为 $V_i$ 在 $K$(表示的基域)上的维数, 则 $d_i \mid |G|$, $d_1^2+\cdots+d_h^2=|G|$[*]. 这当然还不能确定 $d_i$; 但当$|G|$较小的时候, $h$ 由共轭类数确定, $d_i$ 也就可以由此而定. 例如 $G=S_3$, $|G|=6$, 我们知道这时 $h=3$, 那么显然得 $d_1=d_2=1$, $d_3=2$. 这个定理叫做**完备性定理**. 如果这些不可约 $G$-模 $V_i$ 用矩阵表示 $\rho_i$(即线性变换表示)形式写出来: $\rho_i(g)=(a_{kl}^{(i)}(g))$, 右边是依赖于 $g\in G$ 的 $K$ 上的 $d_i\times d_i$ 方阵, $a_{kl}^{(i)}$ 就成为 $G$ 上 $K$ 值函数, 一共是 $d_1^2+d_2^2+\cdots+d_h^2$ 个, 这些函数在 $K$ 上线性无关, 而 $G$ 上所有 $K$ 值函数构成 $K$ 上线性空间 $\mathscr{V}$, $\dim_K\mathscr{V}=|G|$. 所以 $d_1^2+\cdots+d_h^2=|G|$, 就是说 $G$ 上任一 $K$-值函数是 $a_{kl}^{(i)}$ 的 $K$-线性组合,所以叫完备性定理.

---

*) $|G|$是 $G$ 的阶.

常表示理论中的另一个基本定理，叫做**正交性定理**．这是说不可约表示系数函数 $a_{kl}^{(i)}$ 之间的关系．对 $G$ 上 $K$-值函数 $\xi$、$\eta$，定义它们双线性函数 $(\xi, \eta)=\sum\limits_{g\in G}\xi(g)\eta(g^{-1})$，这里求和是 $g$ 跑过 $G$ 中所有元素．于是，这 $|G|$ 个函数 $a_{kl}^{(i)}$ 在这双线性下是互相正交的，即 $(a_{kl}^{(i)}, a_{uv}^{(j)})=0$；除非 $i=j$, $k=u$, $l=v$.

有限群表示的这三个基本定理，也可以推广到紧致连续群的表示上．紧致连续群 $G$ 上可以给出不变积分以代替求和 $\sum\limits_{g\in G}$，于是许多有限群常表示的一些性质可以推过来：

(i) $G$ 的任一有限维表示是完全可约的——表示的完全可约性；

(ii) 设 $(a_{kl}^{(i)}(g))$（这里 $i\in I$ 为指标集）是 $G$ 的不可约表示完全组，则有

$$\int_G a_{kl}^{(i)}(g)a_{uv}^{(j)}(g^{-1})dg=0,$$

除非 $i=j$, $k=u$, $l=v$——这就是正交性；

(iii) 函数 $\Delta=\{a_{kl}^{(i)}\}$ 全体构成 $G$ 上连续函数的均匀完全组，即 $G$ 上每一复值连续函数 $f$ 及每一 $\varepsilon>0$，总存在 $f_1, \cdots, f_n\in\Delta$ 及复数 $\alpha_1, \cdots, \alpha_n$，使

$$\left|f(g)-\sum_{i=1}^{n}\alpha_i f_i(g)\right|<\varepsilon,\ \text{对}\ g\in G.$$

即任一 $G$ 上连续函数都可以用 $\Delta$ 中函数的线性组合来逼近．——这就是完全性．

当 $G=\mathbf{R}/\mathbf{Z}$ 时，关于加法，它是交换的紧致连续群，它的不可约表示都是一维的形式 $\rho_n$: $G\to\mathbf{C}$, $\rho_n(x+\mathbf{Z})=e^{2\pi n x i}$，于是，按上述(iii)（这称为彼得(F. Peter)-外尔定理），$G$ 上任一连续函数 $f$（即实数域上任一周期为 1 的连续函数）均可以用 $\{e^{2\pi n x i}\}$ 的线性组合来逼近，这是古典的调和分析．所以，群上表示的讨论也包含着群上的调和分析．局部紧致群上的调和分析，是当前李群表示论中一个重要方向．另外，紧致群的无限维表示，也是一个重要方向．

不过，这些都已更偏重于分析，特别是泛函分析.

在有限群的常表示理论中，一个问题是怎么能做出不可约表示来. 一个方法是从商群的不可约表示导出来. 设 $N \lhd G$，于是有由 $G$ 到商群 $G/N$ 上的自然同态 $\omega$: $G \to G/N$，显然 $G/N$ 的不可约表示 $\rho$: $G/N \to GL_n(K)$ 都可以得出 $G$ 的不可约表示 $\rho\circ\omega$: $G \to G/N \to GL_n(K)$. 譬如 $N=[G,G]$ 是 $G$ 的换位子群，$G/[G, G]$ 是有限交换群，它的所有不可约表示都是一维的，这样就可以得到 $G$ 的所有一维不可约表示. 另一个办法是对已知的不可约表示做张量积，然后再分解. 另外，还有一个极重要的方法是做诱导，再分解. 所谓**诱导**，就是从 $G$ 的子群 $H$ 的一个表示($H$-模 $W$)做出一个 $G$-模来，记作 $\mathrm{Ind}_H^G W$，称为 $W$ 的诱导表示，这个 $G$-模 $\mathrm{Ind}_H^G W$ 有这样的性质：

(i) 存在 $W$ 到 $\mathrm{Ind}_H^G W$ 内的 $H$-模内射同态 $\varepsilon$: $W \to \mathrm{Ind}_H^G W$；

(ii) 对任一从 $W$ 到 $G$-模 $V$ 的 $H$-模同态 $\xi$: $W \to V$，一定存在从 $\mathrm{Ind}_H^G W$ 到 $V$ 的 $G$-模同态 $\bar{\xi}$: $\mathrm{Ind}_H^G W \to V$，使 $\bar{\xi}\circ\varepsilon=\xi$，即同态图

$$\begin{array}{ccc} W & \xrightarrow{\varepsilon} & \mathrm{Ind}_H^G W \\ & {\scriptstyle\xi}\searrow \quad \swarrow{\scriptstyle\bar{\xi}} & \\ & V & \end{array}$$

为交换图. 诱导 $\mathrm{Ind}_H^G$ 是从 $H$-模范畴到 $G$-模范畴的函子，它的作用很大，对李群与代数群都可以类似地作诱导函子.

## 10. 有限群的模表示理论

早在本世纪初，舒尔(I. Schur)就涉及群的模表示. 但是，系统地、持久地深入研究模表示及其对群结构的应用，那是三十年代从布劳尔开始的. 现在已经成为研究群论必不可少的工具，也可说已经成为一个分支. 所谓有限群 $G$ 的**模表示** $\rho$: $G \to GL_n(K)$，是指基域 $K$ 的特征数 $p$ 数能除尽 $G$ 的阶 $|G|$ 的表示 $\rho$. 模表示的一个特点，是不一定完全可约，即不可分解表示不一定是不可约表

示，因此，在考虑表示的结构时，除了考虑不可约表示之外，还要考虑不可分解表示．布劳尔证明了一个基本性质：群 $G$ 的不可约模表示的个数（等价的算相同）等于 $p$–正则元素的共轭类数．这里，$p$ 是表示的基域 $K$ 的特征数．所谓"$p$–正则元素"，是指阶数不被 $p$ 所整除的元素．所以，不可约的模表示也是有限个，但是不可分解的模表示有无限多，情况要复杂得多．人们首先挑一些主要的来研究．把 $G$ 的正则表示*)的直和分解中所出现的不可分解表示叫做 $G$ 的**主不可分解表示**．可以证明：主不可分解表示的个数 $r$ 恰好等于不可约表示的个数．主不可分解表示 $\rho_i(i=1,\ \cdots,\ r)$ 的合成因子（作为 $G$–模的合成列的合成因子）由 $\rho_i$ 所唯一决定，若其中不可约表示 $\sigma_j(j=1,\ \cdots,\ r)$ 出现的次数为 $c_{ij}$，则 $r$ 阶方阵 $(C_{ij})$ 称为群 $G$ 的嘉当(Cartan)矩阵，它当然与 $p$ 有关．这个矩阵反映群 $G$ 的一些性质，也是模表示理论中研究的一个对象．特别是李型群有它自己特定的内部结构，研究李型群的嘉当矩阵，也是很多人感兴趣的．我国数学家段学复曾用群的模表示理论来探讨单群结构，作出了重要贡献．

## II. 整表示理论

如何作出群 $G$ 的模表示来？通常采取这样一个办法：对 $G$ 的一个不可约的常表示 $\rho$，取一个与 $\rho$ 等价的、系数是"整"的表示，然后把这个表示的所有系数"模 $p$"，就得到一个系数在特征 $p$ 的域上的模表示，这个表示不一定不可约．不可约模表示 $\rho_i$、主不可分解模表示 $\bar{\rho}_i$、不可约常表示 $\sigma_j$ 这三者之间，有一个比较有趣的关系：(i) $\rho_i$ 与 $\bar{\rho}_i$ 是一一对应的；(ii) $\rho_i$ 在 $\sigma_j$ 中出现的重数正好等于 $\sigma_j$ 在 $\bar{\rho}_i$ 中出现的重数，

这种考虑系数在整域上的表示，叫做"整表示理论"．这是表示理论中一个重要方向，它涉及表示理论的许多算术性质，也可看

*) 把 $G$ 的群代数 $KG$ 作为 $G$–模，这样所得的表示叫做 $G$ 的正则表示．

作代数数论的推广，它也是常表示论与模表示论之间的一个桥梁.

## 12. 代数 $K$- 理论进入群论

设 $\Gamma$ 为环，考虑群 $G$ 的系数在 $\Gamma$ 中的所有表示(即 $\Gamma$-自由的 $\Gamma G$-模，凡同构即看作是相同的)，以直和作为加法，成半群；由这半群同通常办法作成加群 $a_\Gamma(G)$（这是以不可分解 $\Gamma G$-模为基的自由加群）. 在 $a_\Gamma(G)$中，以 $G$ 的表示的张量积为乘法，就使 $a_\Gamma(G)$ 成为一个环. $a_\Gamma(G)$实际上是个 $\mathbf{Z}$-代数，把它的系数扩充成 $\mathbf{C}$，得 $\mathbf{C}$-代数 $A_\Gamma(G)=a_\Gamma(G)\otimes_{\mathbf{Z}}\mathbf{C}$，这个环称为 $G$ 的**表示环或格林**(G. Green)**环**. 它实际上是把 $G$ 的所有表示($\Gamma$ 上)放在一起，给以一个代数结构，用以整体地研究 $G$ 的表示. 研究 $A_\Gamma(G)$是研究群 $G$ 的表示的一个重要工具，特别是当 $H\subseteq G$ 时研究 $A_\Gamma(G)$与 $A_\Gamma(H)$之间的关系.

$A_\Gamma(G)$比较大，也较为复杂，对环 $\Gamma G$ 可以相应地做一个另外的环：在以不可分解 $\Gamma G$-模为基的自由加群 $F$ 的元素之间添上这样一些关系：若 $\Gamma G$-模 $M$ 的子模 $N$，商模 $M/N$ 则把 $M$ 与 $N\oplus M/N$ 等同起来，于是可以做出一个加群，记作 $K_0(\Gamma G)$. $F$ 中间的乘法(由模的张量积所引出的)也引出 $K_0(\Gamma G)$ 的乘法. 于是 $K_0(\Gamma G)$成环，称为($\Gamma G$ 的)“格罗森狄克(A. Grothendieck)群”(实际上是环). 这个群的结构也能反映群 $G$ 的 $\Gamma$-表示的许多性质. 这是 $K$-理论中第 0 个群. $K_0$ 是环范畴到交换群范畴的一个函子. 还有 $K_1$ 函子、$K_2$ 函子等等. 而且，这些 $K_i$ 之间有一定的关系. 研究这些 $K_i$ 及其间关系的学科，就叫做**代数 $K$-理论.** 它原始是研究拓扑空间上的纤维丛而得来的.

讨论环 $R$ 上的典型群时，就要研究 $K_1$ 群. $R$ 是一个环，不一定交换. $GL_n(R)$是指系数在 $R$ 中、行列式为 $R$ 中可逆元的所有 $n$ 阶方阵，它是一个群，而且是 $R$ 上的一般线性群. 令 $e_{ij}(r)$ ($i\neq j$)为对角线上全为 1、($i$, $j$)位置上为 $r\in R$、其他位置全为

0的$n$阶方阵；又令$E_n(R)$为由$e_{ij}(r)$ ($i\neq j$, $r\in R$)所生成的$GL_n(R)$的子群. 对于任意$n$,可以把$GL_n(R)$看作$GL_{n+1}(R)$的子群,只要把$g\in GL_n(R)$与$\begin{pmatrix} g & 0 \\ 0 & 1 \end{pmatrix}\in GL_{n+1}(R)$对等起来即可. 于是有

$$GL_1(R)\subseteq GL_2(R)\subseteq\cdots\cdots.$$

同样有

$$E_1(R)\subseteq E_2(R)\subseteq\cdots\cdots.$$

再令$GL(R)=\bigcup\limits_{n=1}^{\infty}GL_n(R)$,它是个群,因为任意两个元素可乘,每个元素有逆元. 它有个子群$E(R)=\bigcup\limits_{n=1}^{\infty}E_n(R)$. 怀特海(J. H. C. Whitehead)证明了:$E(R)$是$GL(R)$的正规子群,而且$K_1(R)=GL(R)/E(R)$是一个交换群,称为"环$R$的$K_1$群",它也是环范畴到交换群范畴的函子,是近代研究典型群的重要工具.

由上知道,$E(R)$是由$e_{ij}(r)$ ($i\neq j$, $r\in R$)所生成的,而这些生成元又满足下列关系式:

(i) $e_{ij}(r)e_{ij}(s)=e_{ij}(r+s)$,其中$i\neq j$;

(ii) $e_{ij}(r)e_{jk}(s)e_{ij}(r)^{-1}e_{jk}(s)^{-1}=e_{ik}(rs)$,其中$i, j, k$互不相同;

(iii) $e_{ij}(r)e_{hk}(s)e_{ij}(r)^{-1}e_{hk}(s)^{-1}=I$,若$j\neq h$、$i\neq k$.

我们知道了生成元和给定的它们间的关系式,就唯一地决定一个群. 凡是具有这些关系式的群,都是它的同态像,这叫做群的表现. 于是,令符号$x_{ij}(r)$ ($i\neq j$, $r\in R$)生成一个满足上述条件(i)、(ii)、(iii)(以$x$代$e$)的唯一的群为$\mathrm{st}(R)$,称为"环$R$的斯坦堡群". 于是,由群的表现的性质,存在满同态$\phi$: $\mathrm{st}(R)\to E(R)$它的核$\ker\phi$称为"环$R$的$K_2$群",记作$K_2(R)=\ker\phi$. st、$K_2$都是函子. 奇怪的是函子$K_0$、$K_1$、$K_2$从不同的角度做出来,但它们间有联系. 还可以对任意$n$定义群$K_n(R)$,得出它们间的关系. 这是奎伦(D.Quillen)的工作,他获得1978年的菲尔兹(J.C.Fields)奖.

# 二、环　论

大家知道，环是具有两个运算（加与乘）的一个代数结构 $R$，它满足(i)加法成交换群；(ii)乘法有结合律；(iii)乘法对加法有分配律．通常碰到的环，一般总假设有乘法单位元素，记作1．具有乘法交换律的环，叫做**交换环**．交换环的标准形象，是整数全体所成的整数环 $\mathbf{Z}$ 与域 $F$ 上一个不定元的多项式全体 $F[x]$．$n$ 阶方阵全体是非交换环的例子．只有有限个元素的环，叫**有限环**．标准的例子是整数模 $n$ 所得的环 $\mathbf{Z}_n=\mathbf{Z}/(n)$．当 $n=p$ 为素数时，$\mathbf{Z}_p$ 是含 $p$ 个元素的有限域，是特征数为 $p$ 的最小的域．所有有限域都是 $\mathbf{Z}_p$ 的有限扩张域，具有 $p^n$ 个元素．这种域也叫做**伽罗瓦域**．元素个数相同的有限域都同构，也即伽罗瓦域由它的元素个数所唯一确定，有时也就记作 $GF(p^n)$．有限域本身的理论不多，但在编码理论、区组设计、组合数学中，非常有用．上面提到的这些有限单群的构作，很多是依赖有限域的．

## 1. 唯一因子分解整域

古典数论实质上是在研究整数环 $\mathbf{Z}$．$\mathbf{Z}$ 有许多基本性质．首先，它是交换环．其次，它没有非零零因子（即若 $a$、$b\in\mathbf{Z}$ 且 $ab=0$，必然有 $a=0$ 或 $b=0$）．这样的环叫做**整域**．凡是整域 $R$，都可以作一个包含 $R$ 的最小域，叫做 $R$ 的**商域**．$\mathbf{Z}$ 的商域就是有理数全体所成的域——有理数域 $\mathbf{Q}$．$\mathbf{Z}$ 还有一个非常重要的基本性质：$\mathbf{Z}$ 中有唯一因子分解，即：任一非零整数 $n$ 都可以唯一地表成素数的乘积 $n=\pm p_1p_2\cdots p_r$，这里 $p_i$ 都是素数，“唯一”是在不考虑因子的次序意义下的．有了它，素数才成为整数环 $\mathbf{Z}$ 在乘法意义下的

基石，每个非零整数 $n$ 可写成 $n=\pm\prod_p p^{\nu_p(n)}$，乘积跑过所有素数 $p$，$\nu_p(n)$是非负整数，它是 $p$ 作为因子在 $n$ 中出现的次数. 如果 $p$ 除不尽 $n$，则 $\nu_p(n)=0$. 同样，对每个非零有理数 $n$，都可唯一地表成 $n=\pm\prod_p p^{\nu_p(n)}$. 这里 $\nu_p(n)$ 可以是任意整数，而且对固定 $n$，几乎所有 $p$ 使 $\nu_p(n)=0$. 于是，对固定 $p$ 给出了映射 $\nu_p$: $\mathbf{Q}^*\to\mathbf{Z}$，这是从非零有理数所成乘法群到加法群 $\mathbf{Z}$ 上的同态. 它还满足

$$\nu_p(a+b)\geqslant\min(\nu_p(a),\ \nu_p(b)),\quad 对\ b\neq -a.$$

这个函数 $\nu_p$ 就称为"有理数域 $\mathbf{Q}$ 的一个**指数赋值**"，它给出了有理数在 $p$ 这一点上的局部特性，也就是表达出素数 $p$ 在有理数中出现的重数. 一个有理数，如果在每个局部 $p$ 都知道它的指数赋值的话，那么这个有理数也就知道了(差一个符号)，这就是

$$n=\pm\prod_p p^{\nu_p(n)}.$$

这里是局部全体决定整体. 这就意味着，它是具有唯一因子分解的整域.

除了 $\mathbf{Z}$ 以外，还有许多具有唯一因子分解的整域. 例如，域上多项式环 $F[x]$、$F[x,y]$(一个变量或多个变量的)等. 怎样的整域具有唯一因子分解？一个重要的充分条件是每两个元素都存在最高公因子，这种整域叫**主理想整域**. 我们知道，如果整环中有类似于 $\mathbf{Z}$ 中的带余式除法(欧几里得算法)，那就可以用辗转相除法求两个元素的最高公因子，这样也就导致唯一因子分解定理的成立. 这种整域，叫做**欧几里得整域**. $\mathbf{Z}$ 与 $F[x]$ 都是欧几里得整域；

$$\mathbf{Z}[i]=\{a+bi\mid a、b\in\mathbf{Z},\ i^2=-1\},$$
$$\mathbf{Z}[\sqrt{2}]=\{a+b\sqrt{2}\mid a、b\in\mathbf{Z}\}$$

也都是欧几里得整域. 人们感兴趣的是哪些是主理想整域而不是欧几里得整域，哪些是有唯一因子分解的整域而不是主理想整域，哪些是不是唯一因子分解的整域，特别是就数的整域而言.

## 2. 主理想整域

代数数的整域中，哪些是主理想整域？这是代数数论中一个主要问题．满足首项为 1 而其他系数在有理数域 $\mathbf{Q}$ 中的多项式的数，叫**代数数**．如果满足首项为 1 而其他系数在 $\mathbf{Z}$ 中的多项式的数，叫**代数整数**．$\mathbf{Q}$ 的有限扩域 $F$ 中每个元素都是代数数，$F$ 就称为**代数数域**，$F$ 中代数整数的全体成一个整域，记作 $O_F$，它就是 $F$ 中整的部分．正像 $\mathbf{Z}$ 在 $\mathbf{Q}$ 中的地位一样，$O_F$ 的商域是 $F$，而且还是整闭的（即：若 $\alpha\in F$，且满足首项为 1 而其他系数在 $O_F$ 中，则 $\alpha\in O_F$）．

主要问题是哪些代数数域 $F$ 有唯一因子分解（指 $O_F$ 有唯一因子分解）？到十九世纪四十年代才明确有些数域中唯一因子分解定理不一定成立，这个问题与古典的费尔马（P. S. Fermat，1601～1665）大定理（$x^n+y^n=z^n$，当 $n>2$ 时没有非零整数解）有关．这里有个故事：1847 年 3 月 1 日法国科学院的会议上，数学家拉梅（G. Lamé）宣称解决了费尔马大问题，并且简约地讲了证明．这当然是件大事，许多数学家上台发言．第一个是刘维尔（J. Liouvill，1809～1882），他没有作肯定的讲话，但是指出不少怀疑之处，其中包括唯一因子分解定理的应用．其次是柯西（A. L. Cauchy，1789～1857）上台讲，他相信拉梅有成功可能性，并说 1846 年 10 月他有报告给科学院，他有一个想法，根据这个想法可以证明费尔马问题，但是没有时间来完成．这次会议之后，拉梅与柯西想尽办法弥补刘维尔所提出的一些疑点，然后宣称他们已有办法对复整数进行因子分解，而且在所做的例子中分解都是唯一的，费尔马问题的证明没有多大障碍了．3 月 15 日的会议上，数学家闻脱兹尔（P. L. Wantzel）宣称已经能证明某些整域的唯一因子分解定理．但是，实际上，他只能解费尔马问题中的 $n\leqslant 4$（这个情况以前已经解决）．对于 $n>4$ 的情况他说可以类推，显然是不对的．几个星期

后，拉梅与柯西各自在科学院的杂志上发表简短的注释，只是很模糊与不完全的，难以令人信服．后来，5 月 24 日刘维尔接到德国数学家库默尔 (E. E. Kummer, 1810～1893) 来信，这场争论才告终．库默尔指出：拉梅的工作中隐含地用了唯一因子分解定理，而这个定理在一般整域中是不一定成立的，并且附上了库默尔在三年前发表过的文章，在那里已经指出拉梅所涉及的一些整域中唯一因子分解不成立．最后，库默尔还说唯一因子分解不成立可以用"理想复数"来代替，这概念已于 1846 年发表在柏林科学院的杂志上．看来是库默尔第一个用"理想"代替"数"，来研究代数数域中唯一因子分解问题．环 $R$ 中的子加群 $I$，如果对任意的 $a\in I$、$x\in R$ 均有 $ax\in I$，则称 $I$ 为 $R$ 的**右理想**；如果对任意的 $a\in I$ 及 $x\in R$ 均有 $xa\in I$，则称 $I$ 为**左理想**；若 $I$ 是 $R$ 的左理想，又是 $R$ 的右理想，则称 $I$ 为 $R$ 的**双边理想**，或就称为**理想**．对交换环来讲，没有左、右理想之分．理想在环中的地位，就像正规子群在群中的地位．一个元素 $a$ 所生成的理想，就叫做**主理想**，记作$(a)$．一个整域 $R$，若 $R$ 中任一理想都是主理想的话，就称为**主理想整域**．如果代数数域 $F$ 的整域 $O_F$ 是主理想整域，那么 $O_F$ 中任意两个元素 $a$ 和 $b$ 所生成的理想$(a, b)$是主理想$(c)$，那么 $c$ 就是 $a$ 与 $b$ 的最大公因子，因此 $O_F$ 有唯一因子分解定理．反之，如果 $O_F$ 有唯一因子分解定理，它一定是主理想整域．

从库默尔的理论可得：设 $p$ 为素数，$\zeta$ 为 $p$ 次单位根，若代数数域 $F=Q(\zeta)$ 的整域 $O_F$ 是主理想整域，那么不定方程 $x^p+y^p=z^p$ 没有非零的整数解．这仅是部分地解决了费尔马问题．

## 3. 戴德金整域

在库默尔之后，戴德金(J. W. R. Dedekind, 1831～1916) 发展了理想的理论．在 $O_F$ 中虽然不一定有唯一因子分解，但是理想的集合可以有唯一因子分解．当然，首先要在环 $R$ 的理想之间

定义乘法：若$\mathscr{A}$、$\mathscr{B}$为$R$中的两理想，则定义$\mathscr{A}\cdot\mathscr{B}=\sum_i a_i b_i$，这是$R$的理想，如果$\mathscr{A}+\mathscr{B}=1$，它就等于$\mathscr{A}\cap\mathscr{B}$. 不能分解（分解时因子不等于自己）的理想称为**素理想**. 于是，就可以证明：在代数数域$F$的整域$O_F$中，每一个理想都可以唯一地（不管因子的次序）分解成素理想的乘积. 如果$O_F$是主理想整域，任一理想都是由一个元素所生成，任一素理想都是一个素元素所生成，于是也就得出了$O_F$的唯一因子分解. 如果我们形式地定义分式理想，对每一素理想$\mathscr{P}$，规定有符号$\mathscr{P}^{-1}$，每个分式理想$\mathscr{A}$可以唯一地表成$\mathscr{A}=\mathscr{P}_1^{\nu_1}\mathscr{P}_2^{\nu_2}\cdots\mathscr{P}_r^{\nu_r}$，其中$\mathscr{P}_1$，$\mathscr{P}_2$，…，$\mathscr{P}_r$为不同的素理想，$\nu_i\in\mathbf{Z}$可正可负. 于是分式理想的全体关于乘法成群. 每一$0\neq\alpha\in F$生成一个主分式理想$(\alpha)=\prod_{\mathscr{P}}\mathscr{P}^{\nu_{\mathscr{P}}(\alpha)}$，其中$\nu_{\mathscr{P}}$是从$F^*=F/\{0\}$到$\mathbf{Z}$的映射，它具有前面提到过的$\nu_p$的性质. 于是，主分式理想的全体在分式理想所成群$\mathscr{F}$中成子群$\mathscr{S}$，商群是个有限交换群，记作$\mathscr{H}=\mathscr{F}/\mathscr{S}$，称为$F$的**(理想)类群**，它的阶$h=|\mathscr{H}|$称为**类数**. 类数$h$与类群$\mathscr{H}$的结构是代数数域$F$的极重要的不变量，它衡量着$F$距具唯一因子分解有多远，$h=1$就是$F$具唯一因子分解. 代数数论的一个重要课题是对各种$F$分析$\mathscr{H}$与计算$h$. 一百多年来，对二次域$F=\mathbf{Q}(\sqrt{d})$（其中$d$为整数同余0或1）研究得较多，当$d>0$时（$F$为实域），$O_F$是欧氏整域*)（从而$h=1$）的有17个. 即$d=5, 8, 12, 13, 17, 21, 24, 28, 29, 33, 37, 41, 44, 57, 73, 76, 97$. 但是$d>0$、$h=1$而不是欧氏整域的有无限多个，最小的一个是53. 而$d<0$、$h=1$的$F=\mathbf{Q}(\sqrt{d})$只有九个，它们是$-3, -4, -7, -8, -11, -19, -43, -67, -169$. 这还是近年来比较突出的结果. 1934年海尔布朗(H. A. Heilbronn)与林福特(E. H. Linfoot)证明了这九个二次域具$h=1$，同时证明了另外最多只有一个虚二次域，而且它的$d$绝对值大于$5\cdot10^9$. 五十年后的今天，贝克尔(A. Baker)证明了这唯一可能的一个也不存在. 贝克尔还

*) 具有带余式除法的整域叫**欧氏整域**.

确定了 $d<0$、$h=2$ 的所有情形. 对于三次数域的类数, 直至现在知道得还不很多, 一般的情况知道得更少, 有著名的西格尔(C. L. Siegel)定理, 说明类数 $h$、判别式 $d$、控制数(*Regulator*) $R$ 这三者当趋向无限大时的关系.

那么, 怎么样的环才有理想的唯一因子分解? 即上述的环 $O_F$ 的哪些特性才使它有理想的唯一分解? 主要是三个:

(i) $O_F$ 是在它的商域 $F$ 中整闭的, 即 $F$ 中关于 $O_F$ 整的元素都在 $O_F$ 中;

(ii) $O_F$ 中素理想都是极大理想, 所谓极大理想 $\mathscr{A}$ 是指 $O_F$ 中只有 $O_F$ 自己是真包含(不等于) $\mathscr{A}$ 的理想, 容易证明极大理想一定是素理想;

(iii) $O_F$ 中的理想满足极大条件, 即若 $\mathscr{A}_1\subseteq\mathscr{A}_2\subseteq\cdots$ 为 $O_F$ 中一个上升链序列, 那么一定存在 $n$, 使得 $\mathscr{A}_i=\mathscr{A}_{i+1}$ 对所有 $i>n$ 成立.

带有理想极大条件的环, 叫诺特环. 这种素理想都极大, 而且在商域中整闭的诺特整域就叫做**戴德金整域**. 在戴德金整域中就可以有理想的唯一因子分解定理. 上述 $O_F$ 是戴德金整域. 一个变量的代数函数域在代数曲线理论中是主要讨论的对象, 它的整域部分也是戴德金整域.

## 4. 诺特整域

满足理想的极大条件的环, 叫**诺特环**. 满足理想的极大条件的整域叫**诺特整域**. 有些诺特整域中没有理想的唯一因子分解定理, 最基本的例子是多个变量的多项式环. 在代数几何的理论中, 经常出现诺特整域, 这是因为二十年代德国女数学家诺特系统地研究了这一类整域以及它们与代数几何的关系才得名的. 在一般诺特整域中, 理想的唯一因子分解不成立, 主要原因之一是素理想

不一定极大. 例如两个变量的多项式环 $F[x_1, x_2]$ 中 ($F$ 为域) 有理想序列 $(0)\subset(x_1)\subset(x_1, x_2)=F[x_1, x_2]$, 这里 $(a_1, \cdots, a_n)$ 表示由元素 $a_1, \cdots, a_n$ 所生成的理想. 由于 $F[x_1, x_2]$ 是整域, 所以 $(0)$ 是素理想, $(x_1)$ 是所有有 $x_1$ 为因子的二变量多项式, 当然是素理想, 且不等于 $F[x_1, x_2]$, 所以素理想 $(0)$ 不是极大理想. 一般地, 如果在诺特整域 $R$ 中有最长可能的素理想序列 $\mathscr{P}_1\subset\mathscr{P}_2\subset\cdots\subset\mathscr{P}_{n+1}$, 则称 $n$ 为 $R$ 的维数. 这个概念正好与 $R$ 所表的几何形象的维数概念一致. 戴德金整域的维数为 1(素理想都极大).

一般诺特整域没有关于素理想的唯一因子分解定理, 但是可以有某种形式的唯一分解, 这是诺特的功绩, 她奠定了代数几何学的代数基础. 交换环 $R$ 中的理想 $q\neq R$, 如果对 $x$、$y\in R$, $x\cdot y\in q$, 总可得或 $x\in q$ 或 $y^n\in q$(对某 $n>0$), 则称 $q$ 为 $R$ 中的**准素理想**. 显然, 素理想是准素理想, 但反之不必然. 譬如, 在 $\mathbf{Z}$ 中一个素数的幂 $p^n$ 所生成的理想 $(p^n)=(p)^n$ 是准素的, 但不是素理想. 但是, 准素理想 $q$ 可以唯一决定一个包含它的最小素理想 $\mathscr{P}=r(q)$. 于是, 有 $\mathscr{P}^n\subseteq q\subseteq\mathscr{P}$(对某个 $n$). 诺特整域的分解定理是: 在诺特整域 $R$ 中, 任一理想 $\mathscr{A}$ 都是有限个准素理想的交 $\mathscr{A}=\bigcap_{i=1}^{n} q_i$, 其中 $q_i$ 为准素理想, 而且, 可以做到

(i) 素理想 $\mathscr{P}_i=r(q_i)$, $i=1, \cdots, n$ 都不相同(如果 $\mathscr{P}_1=\mathscr{P}_2$, 则 $q=q_1\cap q_2$ 也准素, 而且 $r(q)=r(q_1)=r(q_2)$, 于是可以用 $q$ 代替 $q_1\cap q_2$).

(ii) $q_i\not\supset\bigcap_{j\neq i} q_j(1\leqslant i\geqslant n)$, 否则把这个 $q_i$ 去掉就是. 而且素理想 $\mathscr{P}_1, \mathscr{P}_2, \cdots, \mathscr{P}_n$ 由 $\mathscr{A}$ 所唯一确定. 这样, 任一理想就对应一组素理想 $\{\mathscr{P}_1, \cdots, \mathscr{P}_n\}$.

当诺特整域是戴德金时, 即素理想都极大, 而且在商域中整闭, 那么诺特的这一套理论可以推出理想的唯一因子分解, 所以这也是戴德金理论的推广. 它们在代数几何中, 作为主要的代数工具出现.

# 5. 代数几何与交换代数

代数几何与交换代数，简直是难分难解．代数几何研究的对象是代数流形．设 $F$ 是域，集合 $F^n=\{(x_1,\ \cdots,\ x_n)\,|\,x_i\in F\}$ 称为 $F$ 上 $n$ **维仿射空间**，满足若干个 $n$ 变量的多项式 $f_i(X_1,\ \cdots,\ X_n)\in F[X_1,\ \cdots,\ X_n]\,(i=1,\ \cdots,\ m)$ 的点 $x=(x_1,\ \cdots,\ x_n)\in F^n$ 的全体所成的集合 $V_{f_1,\cdots,f_m}=\{(x_1,\ \cdots,\ x_n)\in F^n\,|\,f_i(x_1,\ \cdots,x_n)=0,\ i=1,\ \cdots,\ m\}$，称为 $F$ 上的一个**代数流形**．设多项式 $f_1,\ \cdots,\ f_m$ 在多项式环 $F[X_1,\ \cdots,\ X_n]$ 中所生成的理想为 $\mathscr{A}$，那么 $V_{f_1,\cdots,f_n}$ 中任一点能满足 $\mathscr{A}$ 中任一多项式，事实上，因 $\mathscr{A}=\{g_1f_1+\cdots+g_nf_n\,|\,g_i\in F[X_1,\ \cdots,\ X_n],\ i=1,\ \cdots,\ n\}$，所以有

$$V_{f_1,\cdots,f_n}=\{(x_1,\ \cdots,\ x_n)\in F^n\,|\,f(x_1,\ \cdots,\ x_n)=0,\ 对任一 f\in\mathscr{A}\};$$

反之，$F[X_1,\ \cdots,\ X_n]$ 中任一理想 $\mathscr{A}$ 都是有限生成的：$\mathscr{A}=(f_1,\ \cdots,f_n)$，于是，满足 $\mathscr{A}$ 中所有多项式的点的全体 $V_{\mathscr{A}}$ 就是 $V_{f_1,\cdots,f_n}$．如果先有代数流形 $V=V_{\mathscr{A}}$，考虑所有被 $V$ 中任一点都能满足的多项式全体 $I(V)=\{f\in F[X_1,\ \cdots,X_n]\,|\,f(x)=0,对\ x=(x_1,\cdots,x_n)\in V\}$，显然 $I(V)$ 为 $F[X_1,\ \cdots,\ X_n]$ 中的一个理想，且 $I(V_{\mathscr{A}})\supseteq\mathscr{A}$．如果 $F$ 是代数闭域，那么著名的希尔伯特零点定理说：$I(V_{\mathscr{A}})=\{f\in F[X_1,\ \cdots,\ X_n]\,|\,f^n\in\mathscr{A},对某个\ n\}$．一般地说，不同的理想 $\mathscr{A}_1$、$\mathscr{A}_2$ 可以决定相同的代数流形 $V_{\mathscr{A}_1}=V_{\mathscr{A}_2}$，但是，如果 $\mathscr{A}_1$、$\mathscr{A}_2$ 都有如下性质：$I(V_{\mathscr{A}_1})=\mathscr{A}_1$、$I(V_{\mathscr{A}_2})=\mathscr{A}_2$，这样不同的 $\mathscr{A}_1$ 与 $\mathscr{A}_2$ 就不能决定相同的代数流形．满足 $I(V_{\mathscr{A}})=\mathscr{A}$ 的理想，称为**根理想**．所以，在 $F$ 为代数闭域的情况下，$F[X_1,\ \cdots,X_n]$ 的简约理想与 $F^n$ 中的代数流形一一对应．这是几何形象的代数化的第一步．在这个对应 $V\to I(V)$ 下，代数流形的“联”就对应理想的“乘”，代数流形的“交”对应理想的“和”，大小关系在对应下反过来，素理想对应不可约流形．所谓**不可约流形**，是指这样的代数流

形 $V$，它不能是两个真子流形的联．不可约流形是代数几何研究的基本对象，这是把诺特环的理想的准素分解定理翻译作代数流形的语言而得到的：任一代数流形 $V$ 可以唯一地表示成不可约流形 $V_1, \cdots, V_m$ 的并 $V=V_1 \cup V_2 \cup \cdots \cup V_m$，其中任何一个 $V_i$ 都不包含其他的．

设 $V$ 为代数流形，多项式 $f \in F[X_1, \cdots, X_n]$ 就决定 $V$ 上的函数 $\bar{f}(\bar{f}(x)=f(x)$，对 $x \in V)$，称为 $V$ 上多项式函数．不同的多项式 $f$、$g$ 有可能确定同一 $V$ 上函数 $\bar{f}=\bar{g}$．显然，当且仅当

$$f-g \in I(V)$$

时才有 $\bar{f}=\bar{g}$．因此，$V$ 上多项式函数的全体为

$$F[X_1, \cdots, X_n]/I(V),$$

这是个诺特环，称为"代数流形的仿射坐标环"，记作 $A(V)$．当且仅当 $V$ 是不可约时，$A(V)$ 是诺特整域．

在几何中，研究局部性质占着很重要的位置．反映在代数里，是对局部环的研究．一个交换环 $R$，如果它的非单位元素的全体 $m$ 成理想的话，就称 $R$ 为**局部环**．这时，$m$ 是 $R$ 的唯一极大理想，$R/m$ 是域．反之，如果 $R$ 是具唯一极大理想的交换环，则 $R$ 为局部环．分母不能被素数 $p$（固定）整除的有理数全体是一个局部环；分母不在 $a \in \mathbf{C}$ 处取零值的有理函数 $\dfrac{f(x)}{g(x)} \in \mathbf{C}(x)$ 全体也是一个局部环．设 $R$ 是整域，$F$ 是它的商域，$\mathscr{P}$ 是 $R$ 中素理想，于是

$$R_{\mathscr{P}}=\left\{\frac{b}{a} \middle| a, b \in F, a \notin \mathscr{P}\right\}$$

是一个局部环．对于代数流形 $V$ 来说，仿射坐标环 $A(V)$ 的素理想 $\mathscr{P}$ 代表 $V$ 的闭子流形，极大理想 $m$ 代表 $V$ 的点 $P_m$，于是局部环 $A(V)_{\mathscr{P}}$ 代表子流形附近的性质，$A(V)_m$ 代表点 $P_m$ 处的性质．

代数几何与交换代数关系非常密切，内容很丰富，是当今数学发展中最重要方向之一．

## 6. 非交换代数发展简史

上面谈的，都是交换环的内容. 非交换的环，是不一定满足乘法交换律的环. 环的理论是从代数发展过来的. 所谓 $A$ 是域 $F$ 上的代数(也称 $A$ 是 $F$-代数)，是指：

(i) $A$ 是环;

(ii) $A$ 是 $F$ 上线性空间;

(iii) $\alpha(a\cdot k)=(\alpha a)\cdot b=a\cdot(\alpha b)$，对 $\alpha\in F$，$a$、$b\in A$成立.

代数是数的扩充发展过来的. 是英国数学家哈密顿(W. R. Hamilton, 1805～1865)第一个于 1837 年把复数考虑作为实数对及它们的代数运算，即把复数域 $\mathbf{C}$ 看作是实数域 $\mathbf{R}$ 上的二维代数(这里，维数是指作为域上线性空间的维数). 他研究了实数对的域的运算性质. 然后，他研究三维向量空间的乘法运算是否有类似的域结构，这当然失败了. 然后，转向研究四维的实线性空间. 1843 年 10 月 16 日，他发现了四元数代数，这是个不交换的除环，是人们知道的第一个有限维实可除代数. 后来，弗罗贝尼乌斯证明了它也是除 $\mathbf{R}$ 与 $\mathbf{C}$ 外的唯一的一个有限维实可除代数*). 其实，几乎与哈密顿同时，格拉斯曼(H. G. Grassman, 1809～1877)也考虑了线性空间中的乘法，讨论了代数性质. 他写了一本书，非常长的书名，也非常难懂，没有多少人注意他的工作. 一直到 1878 年，克利福德(W. K. Clifford)的文章发表了，人们才认识它的重要. 现在，人们叫它为格拉斯曼代数与克利福德代数. 相反，哈密顿的思想广泛传播，引起许多人的兴趣，特别 1849 年德·摩根(A. De Morgan, 1806～1871)给出了代数的初步定义，1854 年凯莱(A. Cayley, 1821～1895)的论文中给出了抽象群的定义，还研究了群元素的线性组合所成的集合，也即群代数. 1870 年皮尔斯(B. Pierce)在一篇达 100 页的论文中，系统研究了线性结合代数. 在

*) 可除代数是指代数，同时任一非零元素有乘法逆元；也可叫**除环**.

那里，他引进了幂等元素(即满足 $e^2=e$ 的元素)的概念及皮尔斯分解：代数 $A$ 中若有幂等元素 $e(\neq 0, \neq 1)$，则 $A$ 可以分解成右理想的直和 $A=eA\oplus(1-e)A$；若 $e$ 是中心的(即 $e\in Z(A)$，$A$ 的中心)，则这是双边理想的直和．皮尔斯还引进了幂零元素(即对某 $n$，满足 $x^n=0$ 的元素)的概念．

## 7. 代数的结构

二十世纪初，魏德伯恩(J. H. M. Wedderburn)集大成，在引进代数的根的概念后，给出了代数结构的三个基本定理．

由带算子群的若当-霍尔德定理很容易证明：若代数 $A$ 有右理想及双边理想的直和分解

$A=I_1\oplus I_2\oplus\cdots\oplus I_s$，其中 $I_i$ 为 $A$ 的极小右理想， (1)

$A=J_1\oplus J_2\oplus\cdots\oplus J_r$，其中 $J_i$ 为 $A$ 的极小双边理想， (2)

那么，这样的分解是唯一的(不管直和项的次序，且在同构的意义下)．极小双边理想也叫**单理想**．所谓**单环**，是指除本身与{0}外没有其他理想的环．

什么时侯一个代数 $A$ 可以有上述的分解？一个显然的事实是，如果对 $A$ 的任一右理想 $I$ 总有右理想 $I'$(称为 $I$ 的补)，使 $A=I\oplus I'$，那么 $A$ 就有如(1)的唯一分解；对(2)的分解也是一样．这样的代数 $A$，称为**半单代数**．于是，半单代数是有限个单代数的直和．魏德伯恩对半单代数有个内在的刻划，他给出了代数的根的概念，所谓代数 $A$ 的**根**，是 $A$ 中最大的幂零理想 $R$(幂零是指有 $n$，使 $R^n=\{0\}$)．于是，魏德伯恩的第一定理是：$A$ 为半单代数当且仅当 $A$ 的根 $R=\{0\}$．这时，$A$ 为单代数的直和．一般地，$A/R$ 为半单代数，从而 $A/R$ 是单代数的直和．

魏德伯恩的第三定理是：任一代数闭域 $F$ 上的代数 $A$ 内有半单的子代数 $A'$，使 $A=R\oplus A'$，这里直和是作为 $F$ 上线性空间的

直和. 可惜不是理想的直和, 否则 $A$ 的结构要简单得多了. 由这个定理可知, 一般代数的结构问题可归结为三部份: (i) $R$ 的结构, 这是幂零代数; (ii) $A'$ 的结构, 这可归结为单代数的结构; (iii) $A'$ 以 $R$ 的扩张, 这个分类也是很困难的.

魏德伯恩的第二定理是关于单代数的结构. 令 $\mathfrak{M}_n(R)$ 表示系数在环 $R$ 中的所有 $n$ 阶方阵全体所成的环. 容易证明, 若 $R$ 是除环(每个非零元素都有逆元的环)的话, 则 $\mathfrak{M}_n(R)$ 是单环; 若 $D$ 是可除 $F$-代数, 则 $\mathfrak{M}_n(D)$ 是单 $F$-代数.

## 8. 布 劳 尔 群

魏德伯恩第二定理说, 任一单 $F$-代数 $A$ 都是 $\mathfrak{M}_n(D)$ 形式, 即存在 $n$ 与可除 $F$-代数 $D$, 使 $A\cong\mathfrak{M}_n(D)$, 而且 $n$ 与 $D$ 都由 $A$ 所唯一确定. 这个定理把单代数的结构归结为可除代数的结构. 特别是那些中心为 $F$ 的单 $F$-代数, 称为**中心单代数**, 相应的可除代数为**中心可除代数**, 中心单代数除了 $n$ 外由中心可除代数所唯一确定. 因此, 对中心单代数的研究也就归结为对中心可除代数的研究. 设中心可除代数 $D_1$ 与 $D_2$ 的张量积 $D_1\otimes_F D_2\cong\mathfrak{M}_n(D_3)$, $D_3$ 也是中心可除代数, 如果我们把 $D_3$ 定义作为 $D_1$ 与 $D_2$ 的乘积, 那么布劳尔证明了: 所有 $F$ 上的中心可除代数所成的集合 $B(F)$ 在上述乘法意义下构成一个群(叫做 $F$ 的布劳尔群), 仅依赖于 $F$. 例如 $B(\mathbf{C})=\{e\}$, $B(\mathbf{R})$ 是二阶群. 对局部域 $F$ 的布劳尔群 $B(F)$, 有一个很有趣的结果: $B(F)\cong\mathbf{Q}/\mathbf{Z}$(作为加法群), 它是个无限交换群, 但每个元素都是有限阶的(称为挠群). 其实, 任意域 $F$ 的布劳尔群都是交换挠群. 当 $F$ 是代数数域时 $B(F)$ 可以是无限多个 $\mathbf{Q}/\mathbf{Z}$ 的直和的子群. 布劳尔群的理论非常深入与广泛, 它涉及可除代数的分类、可除代数的伽罗瓦理论、代数的算术理论、伽罗瓦上同调、以及类域论等等.

## 9. 环的结构理论

上面所指的代数，是域 $F$ 上的有限维线性空间，于是，有魏德伯恩结构定理．对一般环，它的结构应如何？是否能有魏德伯恩那样的结构定理？几十年来环论基本上是沿着这条线来发展的．三十年代，阿廷(E. Artin)用环的极小条件*)来代替代数的有限维条件．现在把这种对右(左)理想满足极小条件的环叫做**阿廷环**．在阿廷环 $A$ 中，最大的幂零右(左)理想 $R(A)$ 也是最大幂零双边理想，称为 $A$ 的**根**．对阿廷环 $A$，下述基本性质还是成立的：$A$ 的任一右理想 $I$ 都有补右理想 $J(A=I\oplus J)$ 当且仅当根**) $R=0$．这种环就叫**半单阿廷环**．于是，有阿廷环的结构定理：(i) 任一半单环是单环的直和；(ii) 任一单环 $A\cong\mathfrak{M}_n(D)$，其中 $D$ 为除环，而且 $n$ 与 $D$ 由 $A$ 所唯一确定．任意一个阿廷环 $A$，$A/R(A)$ 是半单的，从而是单环的直和，是一些除环上的全矩阵环的直和．所以，一般阿廷环的结构问题最终归结为幂零环(根)与除环的结构．当然还有一个环扩张的问题，这是阿廷的理论，它扩充了魏德伯恩的结果．

四十年代时，贾柯勃逊(N. Jacobson)更进一步推广了阿廷的结果，把有限性条件(极小条件)去掉了，用本原环的条件来代替单环．容易知道，单环的非零同态总是同构(可以不是满的)，因此单环 $R$ 的不可约 $R$-模 $M$ 总是"忠实的"(即 $a\cdot m=0$，$a\in R$，$m$ 为 $M$ 中任意元素，则 $a=0$)．就把这个作为本原环的定义：若环 $R$ 有一个不可约的忠实 $R$-模，则称 $R$ 为**本原环**．若 $R$ 的理想 $I$ 使环 $R/I$ 为本原环，则称 $I$ 为 $R$ 的**本原理想**；就是说，$R$ 到本原环

---

*) 如果环 $R$ 的任一右(左)理想链 $I_1\supseteq I_2\supseteq\cdots$，一定存在 $n_0$，使当 $n>n_0$ 时有 $I_n=I_{n+1}$，则称 $R$ 满足**右(左)理想的极小条件**．极小条件比极大条件更强些，从极小条件可以推出极大条件，这是霍普金(C. Hopkins)的结果，当然这里所论及的环都是带1的．

**) 阿廷环 $A$ 的根 $R(A)$ 是指 $A$ 的最大幂零右(左)理想，也是最大幂零理想，由极小条件，它一定存在．

上的满同态的核就是本原理想．贾柯勃逊把所有本原理想 $I_\alpha$ ($\alpha \in \Omega$) 的交，$J(R)=\bigcap_{\alpha\in\Omega} I_\alpha$，称为**根**．现在叫**贾柯勃逊根**．贾柯勃逊根 $J(R)=0$ 的环 $R$ 叫贾柯勃逊半单环或半本原环．于是，一个显然的结果是 $R/J(R)$ 是半本原环．根据环的一般理论，任一环 $R$ 中的任一组理想 $I_\alpha$ ($\alpha\in\Omega$)，总有 $R/\bigcap_{\alpha\in\Omega} I_\alpha \cong \coprod_{\alpha\in\Omega} R/I_\alpha$，这里右边是 $R/I_\alpha$ 的亚直和，即全直和 $\prod R/I_\alpha$ 的子环，它到每个 $R/I_\alpha$ 上的射影是满的，这不是一个确定的符号，这里姑且用之．在我们这里，$R/I_\alpha$ 是本原环，于是就得到定理：$R$ 为半本原环当且仅当 $R$ 是本原环的亚直和．这就推广了阿廷半单环的结构定理，结论稍不如人意，因为亚直和不是唯一的．那么，本原环的结构如何？哪些是本原环？对于阿廷环来说，单环与本原环是一致的．对没有极小条件的环来说，就不一样了．例如，除环 $D$ 上的无限维左线性空间 $M$ 中，线性变换 $\varphi$ 的秩 $m$ 是指 $\dim_D\varphi(M)$，那么 $M$ 的所有有限秩线性变换全体 $R$ 是本原环(因为 $M$ 本身就是 $R$ 的忠实不可约模)，由此得在线性变换全体所成的环 $\mathrm{End}_D M$ 中，只要是含 $R$ 的 $\mathrm{End}_D M$ 的子环，都是本原环，所以 $\mathrm{End}_D M$ 也是本原环，但 $R$ 是 $\mathrm{End}_D M$ 的非零真理想，所以，$\mathrm{End}_D M$ 不是单环．但可以证明 $R$ 是个单环．

如果 $R$ 是本原环，按定义，有一个不可约忠实的 $R$-模 $M$，于是 $R$ 可看作 $\mathrm{End}M$ ($M$ 作为加法群的自同态全体所成的环) 的子环，$R$ 在 $\mathrm{End}M$ 中的中心化子 $D=C(\mu)$ 是一个除环，于是 $M$ 是 $D$ 上线性空间，而 $R$ 成为 $\mathrm{End}_D M$ 的子环．另一方面，设有除环 $D$ 上线性空间 $M$，则 $\mathrm{End}_D M$ 上可以给以有限拓扑，如果子环 $R$ 在这个拓扑意义下是稠密的，则称 $R$ 为**稠密环**．贾柯勃逊刻划本原环的定理是：$R$ 为本原环当且仅当 $R$ 为稠密环．$R$ 是含有非零极小右(左)理想的本原环当且仅当 $R$ 是 $\mathrm{End}_D M$ 中含有有限秩线性变换的稠密环，对某除环上的线性变换．进一步对本原环的刻划与分类，至今还有许多人在做工作．复旦大学许永华先生以及他的

学生们在这方面作了许多工作.

## 10. 根　　论

四十年代许多人把根(也即幂零根)的概念推广到一般的环与代数上. 所谓**幂零根**, 是对有限维代数或阿廷环而言, 它是环 $R$ 的最大幂零理想. 对一般环, 有贾柯勃逊根($J$-根). 域 $F$ 上的代数 $A$(不一定有限维)的勒维斯基(J.Levitzki)根($L$-根), 是指 $A$ 的最大局部幂零理想*) $N$; $N=0$ 时就称 $A$ 为 $L$-半单代数, $A/N$ 是 $L$-半单的.

在环 $R$ 中, 使 $R/N$ 没有非零幂零理想的最小理想 $N$, 称为 $R$ 的贝尔(R. Baer)根($B$-根); $N=0$ 时, 就称 $R$ 为 $B$-半单环, $R/N$ 是 $B$-半单的.

环 $R$ 的最大幂零元理想 $N$, 称为 $R$ 的柯特(Koethe)根($K$-根). $N=0$ 时, 称 $R$ 为 $K$-半单环, 而 $R/N$ 是 $K$-半单的.

各种不同的根, 各种不同的“半单环”, 要研究它们的性质与相互关系, 这有助于一般环的分类. 五十年代初, 阿密策(S. A. Amitsur)与库洛什(А.Г.Курош)独立地建立了根的一般理论, 把以前讨论的根都统一于这一般理论下.

把具有某性质 $P$ 的环或理想叫做 $P$-环或 $P$-理想. 如果性质 $P$ 有以下性质:

(i) $P$-环的同态像仍是 $P$-环;

(ii) 任一环 $R$ 有一个最大 $P$-理想 $N$, 它包含 $R$ 的一切 $P$-理想;

(iii) $R/N$ 不含非零 $P$-理想,

则就称 $P$ 为根性质. 其中的 $N$, 就称为环 $R$ 的 $P$-根; $P$-根等于零的环, 就称为 $P$-半单环.

于是, 上述一些根($B$-根, $L$-根, $J$-根, $K$-根)都是由根性质所

*) 局部幂零理想, 是指这理想中任意有限个元素生成的子环都是幂零的.

决定的根.

## 11. 环 模

与群一样，环的表示理论与环模的理论是一致的．环 $R$ 上的左模 $M$ 是指 $M$ 为加法群，$R$ 中每个元素 $a$ 作为 $M$ 的自同态作用在 $M$ 上(以 $a\cdot x$ 记之，其中 $a\in R$, $x\in M$)，并且满足 $(a+b)\cdot x=ax+bx$, $(ab)x=a(bx)$, $1\cdot x=x$. $M$ 称为左 $R$–模．同样，有右模与双边模的定义．如果 $R$ 还是域 $K$ 上代数，那么 $R$–模(左)还要求 $M$ 是 $K$ 上的线性空间，这就是通常的代数表示．环模的理论与环的理论是分不开的.

群的表示理论实际上是环模理论的一部分．因为对群 $G$，可以作它的群代数 $KG$($G$ 的 $K$–线性组合的全体)，而 $KG$–模与 $G$–模是一回事．所以，像群模一样，环模理论最基本的是两个定理：若当–霍尔德定理与克努尔–斯密特 (Krull-Schmidt) 定理．但对一般环模说，后者不一定成立，不是对任意环 $R$ 每一个 $R$–模都可以唯一地分解成有限个不可分解 $R$–模的直和．有些情况下是可以的，那就是定理：若 $R$ 是阿廷环，$M$ 为有限生成 $R$–模*)，则 $M$ 可以唯一地分解成有限个不可分解 $R$–模的直和．这里唯一当然是指不管次序而且是在 $R$–同构的意义下．所以，一般讨论阿廷环 $R$ 上的有限生成模．为了方便起见，下面我们主要谈阿廷代数 $A$，基域 $F$ 是代数闭的，模都是指有限生成 $A$–模.

如果 $A$ 是半单的，模的分类情况比较简单．这时候不可分解模与不可约模一致，不可约模只有限个，它的个数等于 $A$ 的中心 $Z(A)$ 的维数．$A$ 的不可约模都在 $A$ 的正则表示的分解中出现，而且出现的次数正好等于这个不可约模的维数，即若 $V_1$, $V_2$, $\cdots$, $V_h$ 为 $A$ 的所有不同的不可约模，则有

---

*) 有限生成 $R$–模是指这个 $R$–模是由有限个元素所生成的.

$$\sum_{i=1}^{h}(\dim_F V_i)^2=(\dim_F A)^2,\qquad h=\dim_F Z(A).$$

与有限群的常表示情况基本一样，这是因为群代数 $FG$ 是半单阿廷环，所以常表示的一些基本性质可以从半单环理论中套出来.

如果 $A$ 不是半单的，$A$-模的分类就很复杂，像群的模表示论中一样，除了要考虑不可约模外，还要考虑不可分解模. 如果 $A$ 的不可分解模只有有限个(同构算一样)，就称 $A$ 为"有限表示型的代数". 以 $A$ 作为 $A$-模直和分解出的不可分解模，称为"主不可分解模"，它当然只有有限个，它们与不可约模是一一对应的. 主不可分解模有一个重要性质：任一个以主不可分解 $A$-模 $U$ 为同态像的 $A$-模 $M$，必然以 $U$ 为直和项(即若有满同态 $\varphi$: $M\to U$，则 $M\cong U\oplus \mathrm{Ker}\varphi$). 不光是主不可分解模有这个性质. 有这样性质的模，就称为"射影 $A$-模"，与这个概念相对偶的是"内射 $A$-模"：任一含 $A$-模 $V$，作为子模的 $A$-模 $M$，必然以 $V$ 为直和项，(即若 $M\supseteq V$，必存在 $M$ 的子模 $N$，使 $M\cong V\oplus N$)，就称 $V$ 为内射 $A$-模. 内射模与射影模是模论中两个极重要的概念. 射影模的直和项都是射影模，射影模的直和也是射影模，$A$ 本身作为 $A$-模(也叫正则表示)是射影模，若干个 $A$ 的直和 $A\oplus\cdots\oplus A$(作为 $A$-模)也是射影模，这种模称为自由模，$A$ 的个数称为这个自由模的秩. 所以，自由模是射影模；射影模不一定是自由模，但一定是自由模的直和项.

## 12. 环的维数

用以刻划分类环的重要不变量，对交换环 $R$，可以用 $R$ 中素理想链列的长度来定义维数. 对非交换环，通过下列方式来定义：

设 $A$ 为环，$M$ 是有限生成 $R$-模. 一定有一个射影 $R$-模 $C_0$ 及满同态 $\varepsilon$: $C_0\to M$. 这总可做得到，因为 $M$ 是由有限个元素 $x_1$、$x_2$、…、$x_n$ 所生成，我们就可以做一个秩为 $n$，以 $e_1$、$e_2$、…、$e_n$ 为基的

自由 $R$-模 $C$, $C$ 中任一元素 $a\in C$ 可以唯一地表成

$$a=a_1e_1+a_2e_2+\cdots+a_ne_n,\qquad a_i\in R,$$

我们就把这个元素对应到 $M$ 中元素

$$a_1x_1+a_2x_2+\cdots+a_nx_n\in M,$$

这个映射是满的 $A$-同态. 而自由模是射影模. 所以, 一定存在射影模 $C_0$ 及满同态 $\varepsilon$: $C_0\to M$, 不一定就是这个自由模 $C$. 然后, 令 $M_0=\mathrm{Ker}\,\varepsilon$($\varepsilon$ 的核), 再取一个射影模 $C_1$ 及满同态 $d_1$: $C_1\to M_0$, 其核为 $M_1=\ker d_1$, 再取一个射影模 $C_2$ 及满同态 $d_2$: $C_2\to M_1$, 核为 $M_2=\ker d_2$, 如此一直做下去, 得

$$0\longleftarrow M\xleftarrow{\varepsilon}C_0\xleftarrow{d_1}C_1\xleftarrow{d_2}C_2\xleftarrow{d_3}\cdots\cdots. \qquad (*)$$

这是一个带着一连串同态的 $R$-模序列, 它有一个很特殊的性质: 后一个同态的像等于前一个同态的核, 即 $\mathrm{Im}\,d_{i+1}=\ker d_i$. 这样的序列称为**正合列**. 根据上面的做法, 这个序列中除第一个 $R$-模是先给的 $M$ 外, 其他的都是射影 $R$-模. 这样的序列(*)就称为 $M$ 的一个射影分解. 若 $M$ 有一个射影分解(*), 其中 $C_n=0$ 对充分大的 $n$, 那么就称 $M$ 有有限同调维数; 最小的 $n$(在所有 $M$ 的射影分解中)使 $C_n\neq 0$, $C_m=0$, $m>n$, 则称 $n$ 为 $M$ 的**同调维数**, 记作 $h.\dim M$. 显然, $R$-模 $M$ 的同调维数为零当且仅当 $M$ 为射影模. 所以, 模的同调维数描述这个模与射影模相差多远. 对环 $R$, 定义 $R$ 的同调维数(或称整体维数) $r=\sup\limits_{M}h.\dim M$, 其中 sup 表示上确界, $M$ 跑过所有 $R$-模. 对环来讲, 整体维数是个重要不变量. $r=0$ 当且仅当 $R$ 是半单阿廷环; $r\leqslant 1$ 当且仅当 $R$ 是承继环*) (*hereditary ring*). 还可以证明, 若 $F$ 是域, 那么 $n$ 个变量的多项式环 $R=F[x_1, \cdots, x_n]$ 的整体维数 $r=n$, 这正好与通常维数的概念相吻合. 要证明这一点, 不很容易, 要用到同调代数的一些工具. 在深入讨论环的理论中, 同调代数、$K$-理论、范畴理论等都是必不可少的.

---

*) 环 $R$ 称左(右)继承环, 如果 $R$ 中的每一左(右)理想作为 $R$-模是射影的.

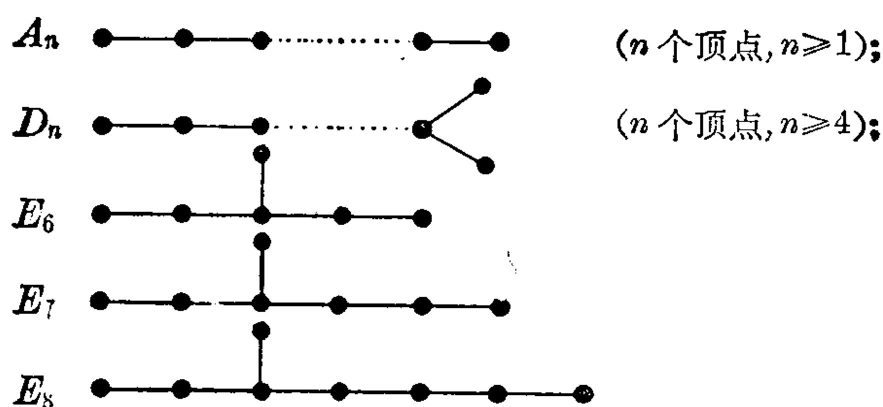
## 13. 代数表示论

作为环论的一部份，近年来，代数的表示理论发展甚为迅猛，内容甚为丰富. 这里，代数一般指的是域 $F$ 上有限维代数 $A$. 如果 $A$ 是半单的，那么 $A$-模的分类、结构都比较简单. 所以，一般是研究非半单的 $F$-代数 $A$，特别着重研究它的不可分解表示. 首先一个问题是什么时候 $A$ 是有限表示型的（即不可分解表示只有有限个），$A$ 的什么性质能反映出 $A$ 是有限表示型？早在 1954 年，希格曼(D. G. Higman)证明了有限群 $G$ 的群代数 $FG$($F$ 的特征数为 $p$)是有限表示型当且仅当 $G$ 的 $p$-西洛(L. Sylow)子群是循环群. 这是一个很有趣的结果. 后来，许多人进一步地研究在这种情况下(有限表示型的群代数)有多少个不可分解表示，它们的结果如何，等等，这些不可分解表示之间的关系常用图(严格说是树)来表达出来，叫做布劳尔树. 这是对群代数而言，而对一般 $F$-代数 $A$ 情况就复杂得多. 设 $A$ 的主不可分解模为 $P_1, P_2, \cdots, P_r$(只有有限个)，对于 $A$，我们可以根据 $P_i$ 的性质做一个有向图*)：取 $r$ 个点对应于不可分解模 $P_1$, $P_2$, $\cdots$, $P_r$; 如果 $\mathrm{Hom}_A(P_i, P_j)\neq 0$，即存在从 $P_i$ 到 $P_j$ 内的非零 $A$-模同态，则从 $i$ 点到 $j$ 点给以一个箭头. 这样组成的有向图，记作 $\Gamma(A)$，称为 $A$ 的箭图(*Quiver*). $\Gamma(A)$只能反映 $A$ 的一部份性质，因为它只用了 $A$ 的主不可分解模之间的关系. 许多不同构的 $F$-代数可以得出相同(或说同构)的箭图. 但是在某一类代数中，箭图却可以刻划出代数 $A$ 是不是有限表示型. 1972 年，伽布里尔(P. Gabriel)证明了这样一个有趣的定理：设 $A$ 为具平方幂零根（即 $J(A)^2=0$）的 $F$-代数，$F$ 代数闭而且 $A$ 的理想所成的格是分配格**)，于是 $A$ 为有限表示型当且仅

*) 有向图就是指由一些点及这些点中间的某些点之间的有向线段所构成的图，如 $\cdot\!\!<\!\!\cdot\!\!\leftarrow\!\cdot$.

**) 这是 $A$ 为有限表示型的必要条件，对任意 $F$-代数都是这样.

当 $A$ 的箭图 $\Gamma(A)$ 的分离图*) $\Gamma^s(A)$ 的无向图是邓金(E. B. Dynkin)图 $A_n$, $D_n$, $E_6$, $E_7$, $E_8$ 的联. 这里 $A_n$, $D_n$, $E_6$, $E_7$, $E_8$ 是指下列这些无向图:




邓金图是用来分类复半单李代数的. 除了上述这些图以外, 还有带双线与三线的图 $B_n=C_n$, $F_4$, $G_2$ 等, 这里出现的恰是所有只含单线的邓金图. 一个是复半单李代数的分类, 一个是有限表示型的分类, 两件互不相关的事却运用了同样的图来分类, 这是很奇妙的现象. 事实上, 近年发现在代数几何学中关于有理奇点的分类, 也运用了邓金图.

我们把代数 $A$ 的不可分解模 $M$ 的合成因子的个数, 叫做"$M$ 的长度", 记作 $l(M)$. 如果 $A$ 的所有不可分解模的长度都小于某一固定数, 则称 $A$ 为"有界表示型的". 四十年代初, 布劳尔与斯拉尔(R. M. Thrall)关于表示型给出了两个著名的猜测:

猜测 1: 有界表示型一定是有限表示型;

猜测 2: 若 $A$ 为无限表示型, 则必有无限个整数 $k$, 使得有无限个不可分解模 $M$ 满足 $l(M)=k$.

通过二十多年许多人的努力, 终于在 1968 年由罗特(A. V. Roiter)解决了猜测 1. 1974 年, 奥斯兰得(M. Auslander)把结果推广到阿廷代数上去. 猜测 2 是 1974 年由纳扎洛瓦(L. A. Nazarova)与罗特所解决的, 只对 $F$ 为代数闭域的情况; 后来, 林

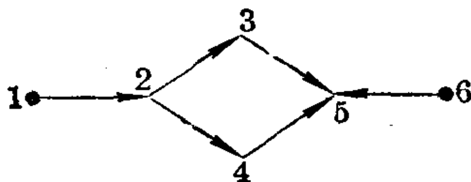
*) 有向图 $\Gamma$ 的分离图 $\Gamma^s$, 是由 $\Gamma$ 通过一个简单的方式做出来的有向图.

格尔(C. M. Ringel)推广到一般域情况.

上面提及从代数 $A$ 作它的箭图 $\Gamma(A)$,虽然这是个有限图,考虑起来方便一点,但这里只用到 $A$ 的主不可分解模之间的联系,不能全面地反映所有不可分解模之间的关系. 七十年代中期,奥斯兰得与瑞托(I. Reiten)把代数 $A$ 的所有不可分解模都取作点(可能有无限多个点),如果在不可分解模 $P_i$ 与 $P_j$ 之间存在不可约映射,就从 $i$ 点到 $j$ 点联一箭头,这样构成一个箭图,称为"奥斯兰得-瑞托箭图",这个箭图的许多状态可以反映出 $A$ 的性质,这是当前非常热门的一个方向.

## 14. 箭图的代数

所谓箭图 $\Gamma$,就是有向图,就是给出点的集合 $V$ 及点对的集合 $E$,$(i,\ j)\in E$ 表示从点 $i$ 到点 $j$ 有箭头. 所以表成 $\Gamma=(V,E)$. 如果按着箭头方向(要一个接一个连接上)能从 $i$ 点到 $j$ 点,这样的一个通路叫做 $\Gamma$ 中从 $i$ 到 $j$ 的一个道路,例如箭图




从 1 到 3 有一个道路,从 1 到 5 有两个道路,而从 1 到 6 就没有道路. 把箭图 $\Gamma$ 的所有道路(任何起点与终点)作基,做一个域 $F$ 上的线性空间 $Q(\Gamma)$;然后,基之间定义乘法:设 $\Gamma$ 中道路 $A$ 与 $B$,如果 $A$ 的终点就是 $B$ 的起点,那么就定义乘积 $A\cdot B$ 为把 $A$ 与 $B$ 接起来的那个道路,否则就定义 $A\cdot B=0$. 这样,显然成一 $F$-代数,称为 $\Gamma$ 的**道路代数**. 道路代数的性质、分类等,也是当前研究的一个方向. 道路代数的表示理论与箭图的表示理论是一致的. 所谓箭图 $\Gamma=(V,E)$的一个表示,是指对任一 $i\in V$,给一个线性空间 $V_i$,对任一箭头 $(i,\ j)\in E$ 给一个从 $V_i$ 到 $V_j$ 的线性变换,这样就给出了 $\Gamma$ 的一个表示. 当然还要定义表示的等价、直和、

子表示等概念. 于是, $\Gamma$ 的表示成一范畴, 这个范畴与 $\Gamma$ 的道路代数的模范畴等价。

## 15. 李 代 数

上面介绍的都是结合代数, 就是乘法满足结合律的. 通常代数就是指结合代数. 非结合代数是指乘法不满足结合律的线性空间, 但一般总还有一个关系式来代替乘法结合关系, 乘法关于加法的分配律总是成立的.

域 $F$ 上的线性空间 $L$, 对 $x$、$y\in L$ 有乘法 $[x, y]\in L$, 它满足

(i) 运算 $[x,y]$, 对 $x$ 与 $y$ 而言都是线性的(这就是分配律);

(ii) $[x, y]=-[y, x]$, 对所有 $x$, $y\in L$.

(iii) $[x, [y, z]]+[y, [z, x]]+[z, [x, y]]=0$, 对所有 $x$, $y$, $z\in L$.

于是, $L$ 就称为 $F$ 上的**李代数**. 它关于 $F$ 的维数, 可以是有限, 也可以是无限, 下面主要谈有限维的. 李代数是由于研究李群的需要而产生与发展的. 李代数虽然乘法没有结合律, 但是依靠了性质(iii)(称为雅可比(C. G. J. Jacobi)等式), 一些基本概念与性质: 子代数、理想、商代数、直和、可解、幂零等等, 都与结合代数一样可定义. 于是, 李代数 $L$ 的最大可解理想 $R(L)$ 就称为 $L$ 的根, 根为零的李代数叫做半单李代数; $L/R(L)$ 是半单李代数; 半单李代数是单李代数(没有非显然理想的李代数)的直和. 任意一个李代数 $L$ 都有一个半单子代数 $S$ 使得 $L=S\oplus R(L)$, 作为线性空间直和. 这些都与结合代数中的魏德伯恩定理一样. 关键是单李代数怎么分类, 什么结构. 复数域上的单李代数的分类、构造, 早在本世纪初, 就由嘉当所解决, 分成四大类与五个特殊代数: $A_n(n\geqslant1)$, $B_n(n\geqslant2)$, $C_n(n\geqslant3)$, $D_n(n\geqslant4)$, $E_6$, $E_7$, $E_8$, $F_4$, $G_2$. 后来, 邓金把这些代数用图表达出来, 就是前面所提到过的邓金图. 由邓金图, 可以给出相应的所谓嘉当矩阵. 由这个矩阵, 就可以做

出相应的单李代数，这个代数的乘法表全部写得出．对复单李代数，不光是分类、结构知道得清楚，而且它们的表示也完全清楚．对实单李代数的分类、结构，也已于 1939 年由甘特马赫(F. Gantmacher)所解决．

近年来，由凯斯(V.Kac)与莫德(R.V.Moody)所独立构作起的一类李代数(一般无限维的)受到各方面的注意，现在叫做"凯斯-莫德李代数"，它与物理学有着密切的联系，与微分方程、组合数学、群论等也都有联系，形成了一个很重要的分支．

上面所谈到的主要是特征数零的李代数．对于特征数 $p$ 的单李代数的分类，是长远以来未解决的问题．但是，特征数 $p$ 的李代数中的一类李代数，叫做限制李代数，这种单李代数的分类是最近才彻底解决的(长达几十年才解决，也成了数学界的一件大事)．

# 三、域　论

## 1. 域的一些基本性质

**域**是一个交换环，而且每一非零元素都有逆元素．所以，域 $F$ 中所有非零元素全体 $F^*$ 构成一个乘法交换群．最小的正整数 $n$ 使 $n\cdot 1=0$ 的必为素数 $p$，$p$ 称为 $F$ 的**特征数**．如果没有正整数 $n$ 使 $n\cdot 1=0$，则称 $F$ 的"特征数为零"．整数环 $\mathbf{Z}$ 的商环 $\mathbf{Z}/p\mathbf{Z}$ 就是一个特征数为 $p$ 的最小域，记作 $F_p$；任一个特征数 $p$ 的域都包含 $F_p$．有理数域 $\mathbf{Q}$ 是特征数 0 的最小域，任一特征数 0 的域都包含 $\mathbf{Q}$．如果两个域 $K\supseteq F$，则称 $K$ 为 $F$ 的**扩域**，$F$ 为 $K$ 的**子域**．于是，$K$ 是 $F$-线性空间；若 $\dim_F K<\infty$，则称 $K$ 为 $F$ 的有限扩张($\dim_F K$ 称为次数，记作 $[K:F]$．此时，$K$ 中每一元素关于 $F$ 都是代数元素(即能满足多项式 $x^n+a_1x^{n-1}+\cdots+a_n$，其中

$a_i \in F,\ n \geqslant 0$). 如果 $F$ 的扩域 $K$ 中的任一元素都是代数元素(关于 $F$), 则称 $K$ 为"**$F$ 的代数扩域**". 所以, 有限扩域都是代数扩域; 反之不尽然. 例如, 代数数的全体是有理域 $\mathbf{Q}$ 上的代数扩域, 但不是有限扩域. 对任意域 $F$, 总可以做一个域 $\overline{F}$, 使得 $\overline{F}$ 是 $F$ 的代数扩域, 而不存在真包含 $\overline{F}$ 的 $F$ 的代数扩域, 称 $\overline{F}$ 为"**$F$ 的代数闭包**". 这时候, $\overline{F}$ 是个代数闭域, 即它不存在真包含它的代数扩域.

## 2. 一般伽罗瓦理论

伽罗瓦理论起源于研究方程的根. 从本质上看, 它实质是用域的自同构群来研究代数扩域. 设 $K$ 为域 $F$ 的扩域, 凡使 $F$ 中元素不变的 $K$ 自同构, 称为"$K$的 $F$-自同构". 显然, $K$ 的 $F$-自同构全体成群, 称为"$K$ 关于 $F$ 的伽罗瓦群", 记作 $\mathrm{Gal}(K/F)$. 令 $K$ 的所有自同构全体所成的群为 $\mathrm{Aut}(K)$. 设 $\Gamma$ 为 $\mathrm{Aut}(K)$ 的子群, 则 $K$ 中被 $\Gamma$ 所不变的元素全体 $\mathrm{Inv}(\Gamma)$ 成 $K$ 的子域, 称为"$\Gamma$ 的不变子域". 于是, 显然有:

(i) 若域 $P \subseteq Q \subseteq K$, 则 $\mathrm{Gal}(K/P) \supseteq \mathrm{Gal}(K/Q)$;

(ii) 若群 $\Gamma \subseteq \Delta \subseteq \mathrm{Aut}(K)$, 则 $\mathrm{Inv}\Gamma \supseteq \mathrm{Inv}\Delta$;

(iii) 若域 $P \subseteq K$, 群 $\Gamma \subseteq \mathrm{Aut}(K)$, 则 $\Gamma \subseteq \mathrm{Gal}(K/P) \Leftrightarrow P \subseteq \mathrm{Inv}(\Gamma)$;

(iv) 若域 $P \subseteq K$, 则 $P \subseteq \mathrm{Inv}(\mathrm{Gal}(K/P))$,

(v) 若 $\Gamma \subseteq \mathrm{Aut}(K)$, 则 $\Gamma \subseteq \mathrm{Gal}(F/\mathrm{Inv}(\Gamma))$.

总之, 在集合{$K$ 的子域}与{$\mathrm{Aut}(K)$的子群}之间, 有两个映射 $\xi$ 与 $\theta$:

$$\{K \text{ 的子域}\} \underset{\theta}{\overset{\xi}{\rightleftarrows}} \{\mathrm{Aut}(K)\text{的子群}\},$$

$$\xi(P) = \mathrm{Gal}(K/P), \qquad \theta(\Gamma) = \mathrm{Inv}(\Gamma),$$

它们使大的对应小的, 小的对应大的, $\theta\xi(P) \supseteq P$, $\xi\theta(\Gamma) \supseteq \Gamma$. 于

是，即得 $\theta\xi\theta(\Gamma)=\theta(\Gamma)$，$\xi\theta\xi(P)=\xi(P)$ 对任意 $K$ 的子域 $P$ 与任意 $\mathrm{Aut}K$ 的子群 $\Gamma$ 成立．$\xi$ 与 $\theta$ 不是互逆的，不是一一对应的关系，但是，限于 $\{\theta(\Gamma)\mid\Gamma\subseteq\mathrm{Aut}K\}$ 与 $\{\xi(P)\mid P\subseteq K\}$ 是一一对应的，$\xi$ 与 $\theta$ 就是互逆的．我们就把这种 $\Gamma=\xi(P)\subseteq\mathrm{Aut}(K)$，称为"$K$ 上的伽罗瓦群"；这种 $P=Q(\Gamma)\subseteq K$，称为"$K$ 中的不变子域"，于是，对域 $K$ 来讲，$K$ 上伽罗瓦群与 $K$ 中的不变子域之间构成一一对应关系，小的对应大的，大的对应小的．这种对应关系就叫做伽罗瓦对应．这是对一般域都适用的一般伽罗瓦理论．

## 3. 有 限 域

有限个元素的域 $F$ 就叫**有限域**，它一定是特征数为 $p$ 的，因此 $F\supseteq\mathbf{F}_p$（$p$ 个元素的素域），而且 $[F:\mathbf{F}_p]=n<\infty$，即 $\dim_{\mathbf{F}}F=n$．因此 $|F|=p^n$，有限域中元素的个数，一定是素数幂．而且，元素数唯一确定有限域（同构作为相同），每个素数幂对应有唯一的一个有限域．设 $K\supseteq F$ 是两个有限域，$[K:F]=m$，$|F|=p^n$，$|K|=p^{mn}$．于是 $K$ 关于 $F$ 有这样性质：$\mathrm{Inv}(\mathrm{Gal}(K/F))=F$．有这样性质的域叫做"$K$ 关于 $F$ 是正规的"．再加上 $K/F$ 是可分*)的和 $[K:F]=m<\infty$，运用一般的伽罗瓦对应，就可得出 $\mathrm{Gal}(K/F)$ 的子群 $\Gamma$ 与 $K$、$F$ 之间的中间域 $P(K\supseteq P\supseteq F)$ 一一对应．而我们知道 $\mathrm{Gal}(K/F)$ 是个 $m$ 阶的循环群 $\langle\sigma\rangle$，这里 $\sigma$ 是使 $F$ 中元素不变的 $K$ 的自同构：$\sigma(x)=x^{p^n}$（对任 $x\in K$）．所以 $\mathrm{Gal}(K/F)$ 有多少子群，子群的结构完全清楚，从而 $K\supseteq F$ 之间有多少中间域，这些中间域的结构也完全清楚．

因此，有限域的结构比较容易掌握．有限域在组合数学，特别是区组设计、有限几何、编码理论中，有很多用处．

---

*) 代数元素 $\alpha\in K$ 称为"关于 $F$ 是可分的"，如果 $\alpha$ 关于 $F$ 的最小多项式没有重根．$K/F$ 称为"可分的"，如果 $K$ 中每一元素关于 $F$ 是可分的．

## 4. 代数数域

域中研究得最多的是**代数数域**，也叫**数域**，这是由于它实质上是数论的一部份．所谓代数数域，就是有理数域 $\mathbf{Q}$ 的有限扩域 $K$．可以证明，这种有限扩域都可以由一个元素 $\theta$ 所生成，即 $K=\mathbf{Q}(\theta)$．于是 $[K:\mathbf{Q}]$ 就等于 $\theta$ 的最小多项式 $f(x)$ 的次数．如 $f(x)$ 的根全都在 $K$ 中，则称 $K$ 为 $\mathbf{Q}$ 的**正规扩张**，或**伽罗瓦扩张**．这时，$\mathbf{Q}=\mathrm{Inv}(\mathrm{Gal}(K/\mathbf{Q}))$，$G=\mathrm{Gal}(K/\mathbf{Q})$ 即为使 $\mathbf{Q}$ 中元素不变的 $K$ 的自同构．于是 $K$ 与 $\mathbf{Q}$ 之间的中间域 $F$ 与 $G$ 的子群 $H$ 一一对应，$F$ 对应 $\mathrm{Gal}(K/F)$，$G$ 的子群 $H$ 对应 $\mathrm{Inv}H$，而且

$$\mathrm{Inv}(\mathrm{Gal}(K/F))=F,\qquad \mathrm{Gal}(K/\mathrm{Inv}H)=H.$$

设 $K$ 是 $\mathbf{Q}$ 的伽罗瓦扩张，如果 $\mathrm{Gal}(K/\mathbf{Q})$ 是循环群（交换群），则称 $K$ 为**循环（交换）扩张**．

对数域 $K$ 来讲，最重要的是研究它的整域部份的性质．$K$ 中的代数整数全体成一整域，记作 $O_K$．若有 $\mathbf{Q}\subseteq F\subseteq K$，则有 $\mathbf{Z}\subseteq O_F\subseteq O_K$，$O_F=O_K\cap F$，$O_K$ 作 $\mathbf{Z}$-模是自由的．$O_K$ 是戴德金环，它的理想有唯一因子分解，基础是 $O_K$ 中的素理想．$K$ 中分式理想全体成乘法交换群，它商掉 $K$ 中主分式理想所成子群就得 $K$ 的类群．类群的研究，是代数数论的主要课题之一．$\mathbf{Q}\subseteq F\subseteq K$ 为数域，设 $\mathscr{P}$ 为 $O_F$ 中一个素理想，$\mathscr{P}$ 在 $O_K$ 中生成一个理想 $\mathscr{P}O_K$，它在 $O_K$ 中不一定是素理想，希尔伯特理论告诉我们 $\mathscr{P}O_K$ 在 $O_K$ 中怎么分解：若数域 $K$ 是 $F$ 的正规扩张，则 $\mathscr{P}O_K=(\overline{\mathscr{P}}_1\overline{\mathscr{P}}_2\cdots\overline{\mathscr{P}}_g)^e$，其中 $\overline{\mathscr{P}}_1,\cdots,\overline{\mathscr{P}}_g$ 为 $O_K$ 中素理想（有 $\overline{\mathscr{P}}_i\cap O_F=\mathscr{P}$），

$$efg=[K:F]=|\mathrm{Gal}(K/F)|,\ f=[O_K/\overline{\mathscr{P}}_i:O_F/\mathscr{P}],$$

这里 $\overline{\mathscr{P}}_i$，$\mathscr{P}$ 各是 $O_K$ 与 $O_F$ 中素理想，为极大理想，所以 $O_K/\overline{\mathscr{P}}_i$、$O_F/\mathscr{P}$ 都是域，而 $O_F\to O_K$ 嵌入映射导出域的嵌入：$O_F/\mathscr{P}\to O_K/\overline{\mathscr{P}}_i$．$e$ 称为分歧数，若 $e=1$ 则称"素理想 $\overline{\mathscr{P}}_i$ 是不分歧的"或"$\mathscr{P}$ 不分歧"．根据戴德金的理论，分歧的理想只有有限个．

# 5. 赋 值 论

素理想是数域的算术理论的基础．但是，我们可以用赋值来代替．赋值理论已成为代数数论与代数函数论的重要工具，而且，它本身也已成为代数中的一个分支．

域 $K$ 的赋值 $\varphi$ 是映射：$K\to\mathbf{R}$，它满足

（i）$\varphi(a)\geqslant 0$，等于 0 当且仅当 $a=0$；

（ii）$\varphi(ab)=\varphi(a)\varphi(b)$，$a$、$b\in K$；

（iii）$\varphi(a+b)\leqslant\varphi(a)+\varphi(b)$，$a$、$b\in K$．

如果对任意 $a$、$b\in K$，有 $\varphi(a+b)\leqslant\max(\varphi(a),\ \varphi(b))$，以此代替(iii)所得的赋值 $\varphi$，称为"非阿基米得赋值"；否则，称为"阿基米得赋值"．由这个定义，直接可推出：域 $K$ 有了赋值 $\varphi$，就在 $K$ 上给出了一个尺度（*metric*），从而使 $K$ 成为一个拓扑空间，成为一个拓扑域．如果 $K$ 上两个赋值 $\varphi_1$ 与 $\varphi_2$ 在 $K$ 上给出的拓扑是一致的话，就称"$\varphi_1$ 与 $\varphi_2$ 等价"．赋值的等价类，就称为 $K$ 的一个位（*place*），我们仍以赋值 $\varphi$ 表示．对有理数域 $\mathbf{Q}$ 来讲，非阿基米得赋值（或位）与素数相当，一一对应．对素数 $p$，可以作一个 $\mathbf{Q}$ 的非阿基米得赋值 $\varphi_p$：设有理数 $a\neq 0$ 写成因子分解形式 $a=\pm\prod\limits_q q^{\nu_q(a)}$，其中 $q$ 跑过所有素数，$\nu_q(a)$ 表示 $a$ 中出现 $q$ 的次数，可正、可负、也可以是 0，而且是除有限个 $q$ 外 $\nu_q(a)$ 都是零，所以乘积是有意义的．于是，令 $\varphi_p(a)=\dfrac{1}{p^{\nu_p(a)}}$，当 $a\neq 0$ 时；而 $\varphi_p(0)=0$．可以证明：$\varphi_p$ 是 $\mathbf{Q}$ 的非阿基米得赋值，而 $\mathbf{Q}$ 的任一个非阿基米得赋值都与适当的 $\varphi_p$ 等价，因此非阿基米得位与素数全体（也即 $\mathbf{Q}$ 的素理想全体）一一对应．在 $\mathbf{Q}$ 上取绝对值（$\varphi_\infty(a)=|a|$，$a\in\mathbf{Q}$）是 $\mathbf{Q}$ 的唯一的一个阿基米得位，任一阿基米得赋值都与绝对值赋值等价（在 $\mathbf{Q}$ 上）．绝对值的这个位叫做 $\infty$ 位，其他的 $\varphi_p$ 是有限位．这是 $\mathbf{Q}$ 的情况，代数数域 $K$ 的情况也相类似：$O_K$ 的素理想与 $K$ 的

非阿基米得等价类(有限位)一一对应，但 $\infty$ 位有 $r_1+r_2$ 个，其中 $r_1$、$r_2$ 表示 $\mathbf{C}$ 中含有 $r_1$ 个与 $K$ 同构的实域(仅含实数的域)及 $r_2$ 个与 $K$ 同构的复域(含有复数的域)．对 $O_K$ 中一个素理 $P$，对应 $K$ 的唯一的位 $\mathscr{P}$，可以取一个标准的赋值，记作 $\varphi_{\mathscr{P}}$．函数 $\varphi_{\mathscr{P}}$ 完全反映出 $K$ 在 $\mathscr{P}$ 位处的局部性质，集合 $\{a\in K \mid \varphi_{\mathscr{P}}(a)\leqslant 1\}=\sigma_{\mathscr{P}}$ 是一个环，表达出 $K$ 在 $\mathscr{P}$ 位处的整域，它是一个局部环(有唯一极大理想的环)，它的极大理想为 $\{a\in K \mid \varphi_{\mathscr{P}}(a)<1\}=I_{\mathscr{P}}$, $I_{\mathscr{P}}\cap O_K=\mathscr{P}$．赋值代替素理想，还可以表达出素理想在扩域中的分解．设 $K\supseteq F$ 为数域，$\overline{\mathscr{P}}$ 为 $K$ 中素理想，对应于赋值 $\varphi_{\overline{\mathscr{P}}}$，$\varphi_{\overline{\mathscr{P}}}$ 是 $K$ 上函数，把它局限于 $F$，就得 $F$ 的赋值 $\varphi$，于是 $\varphi$ 所对应的 $F$ 中素理想 $\mathscr{P}$，恰好 $\overline{\mathscr{P}}$ 就是 $\mathscr{P}O_k$ 的因子．因此，关于素理想在扩域中分解的理论，都可以用赋值来说明．

关于赋值，有一个基本定理，叫做逼近定理，它是孙子定理(又称中国剩余定理)的翻版．这定理说：给出 $n$ 个整数 $\alpha_1, \cdots, \alpha_n$ 及 $n$ 个不同素数 $p_1, \cdots, p_n$，以及 $n$ 个正实数 $\varepsilon_1, \cdots, \varepsilon_n$，则总存在 $\alpha\in \mathbf{Z}$，使

$$\varphi_{p_i}(\alpha-\alpha_i)<\varepsilon_i, \qquad \text{对 } i=1, \cdots, n.$$

这与孙子定理完全一样．逼近定理还可以更一般些，为强逼近定理，成为类域论中的一个基本定理．

赋值论不仅被数域、代数函数域、代数几何等作为基本工具来应用，而且本身也已发展成一个分支．

## 6. 整体域，局部域

数域 $K$ 上的赋值 $\varphi_{\mathscr{P}}$($\mathscr{P}$ 可以有限，也可以无限)既然在 $K$ 上给出尺度，$K$ 成为一个拓扑环，就可以考虑它的完备化；正像绝对值给出 $\mathbf{Q}$ 上的一个尺度，$\mathbf{Q}$ 按照这个尺度做完备域就是实数域 $\mathbf{R}$，这是十九世纪柯西构造实数的办法．对于数域 $K$ 来讲也是一样：称 $K$ 中序列 $\{a_n\}$ 为柯西序列，如果对 $\varepsilon>0$，存在 $n_0$，使当 $n$、$m$

$>n_0$ 时，总有 $\varphi_{\mathscr{P}}(a_n-a_m)<\varepsilon$. 对柯西序列，定义“加”和“乘”：

$$\{a_n\}+\{b_n\}=\{a_n+b_n\}, \qquad \{a_n\}\cdot\{b_n\}=\{a_nb_n\}.$$

如果对 $\varepsilon>0$，存在 $n_0$，使 $\varphi_{\mathscr{P}}(a_n)<\varepsilon$ 对所有的 $n>n_0$ 成立，则称序列 $\{a_n\}\to 0$(趋于 0). 于是，$K$ 中所有柯西序列所成集合 $K'$ 成环，其中极限为零的序列是 $K'$ 的极大理想，$K'/K=K_{\mathscr{P}}$ 是域. $a\in K$ 可看作序列 $\{a\}$ ($a_n$ 都等于 $a$)，这样 $K$ 就成为 $K_{\mathscr{P}}$ 的子域；而且，$K$ 的赋值 $\varphi_{\mathscr{P}}$ 可以唯一地扩充成 $K_{\mathscr{P}}$ 的赋值，仍记作 $\varphi_{\mathscr{P}}$. 这时候，$K_{\mathscr{P}}$ 在赋值 $\varphi_{\mathscr{P}}$ 的拓扑下是一个完备空间. 当 $\mathscr{P}$ 有限时 (即 $\mathscr{P}$ 为 $K$ 中素理想)，称 $K_{\mathscr{P}}$ 为 $\mathscr{P}$-adic 域；$\mathscr{P}$ 无限大位时，$K_{\mathscr{P}}$ 为实数域 $\mathbf{R}$ 或复数域 $\mathbf{C}$. 这些都是局部域，意思是 $K$ 局部化之后的域，它反映 $K$ 在 $\mathscr{P}$ 位处的局部性质. 局部域的一般定义是：非离散的局部紧的拓扑域. 可以证明，局部域只有两大类，一类是特征零的，它是数域 $K$ 所做出的 $\mathscr{P}$-adic 域 $K_{\mathscr{P}}$ 与 $\mathbf{R}$ 及 $\mathbf{C}$；另一类是特征数 $p$ 的，它是有限域 $F_q$ 上的一个变量代数函数域 $\mathbf{F}_q(t)(\theta)=K$ 的素理想位 $\mathscr{P}$ 处所做完备化 $K_{\mathscr{P}}$(这时，所有位都是非阿基米得的). 这两类域 (数域 $Q(\theta)$ 与有限域 $\mathbf{F}_p$) 上一个变量 $t$ 的代数函域 $\mathbf{F}_q(t)(\theta)$，统称为“整体域”. 它们不仅在局部性质上有类似的拓扑结果，而且，在整体上也有许多类似的地方. 最基本的一个性质是它们都有“乘积公式”：对于 $Q\in K^*$($K$ 中非零元素)都有

$$\prod_{\mathscr{P}}\varphi_{\mathscr{P}}(a)=1,$$

其中 $\mathscr{P}$ 跑过 $K$ 的所有位(有限的及无限的). 还可以把 $K$ 的所有局部域并在一起，做出由 $K$ 决定的两个极重要的交换群：Adele 环 $A_K$ 与 idélé 群 $J_K$. 这是反映整体域的整体性质的群，它们的结构包含着 $K$ 的许多算术性质，是研究代数数论与类域论的极重要工具. 设 $K$ 为数域，$\mathfrak{S}=$ 所有 $K$ 的位 $=\{\mathscr{P}\}$，$S_\infty$ 为所有阿基米得位(赋值)全体，对 $O_K$ 中素理想 $\mathscr{P}$，$K_{\mathscr{P}}$ 为相应的局部域，$v_{\mathscr{P}}=\{\alpha\in K_{\mathscr{P}}\mid\varphi_{\mathscr{P}}(\alpha)\leqslant 1\}$ 是相应的局部整域，它的唯一极大理想是主理想 $m_{\mathscr{P}}=(\pi_{\mathscr{P}})$. 设 $\mathfrak{S}\supset S\supseteq S_\infty$，且 $S$ 为有限集. 于是，定义

$$A_k(S)=\prod_{\mathscr{P}\in S}K_{\mathscr{P}}\times\prod_{\mathscr{P}\notin S}v_{\mathscr{P}},\qquad A_k=\bigcup_{s}A_k(s).$$

容易看出，$A_k$ 根据坐标各自相乘相加的办法定义乘与加，于是 $A_k$ 成环，叫做 $K$ 的 Adele 环，元素都叫 Adele. $A_k$ 作为环，其中单位的全体成乘法交换群，叫做 $K$ 的 idélé 群. 再在 $A_k$ 与 $J_k$ 中各自定义拓扑，使 $A_k$ 与 $J_k$ 成拓扑环与拓扑群，都是局部紧的. $K$ 可以对角地嵌入于 $A_k$ 中，即对 $a\in K$ 可作 $i(a)=\prod_{\mathscr{P}\in\mathfrak{S}}i(a)_{\mathscr{P}}$，其中 $i(a)_{\mathscr{P}}=a\in K_{\mathscr{P}}$，对每个 $\mathscr{P}\in\mathfrak{S}$. 同样，$K^*$ 可以对角地嵌入 $J_k$ 中. 有趣的是，$K$ 是 $A_k$ 中的离散子群(对加法而言)，而 $A_k/K$ 是紧致的拓扑群(从 $A_k$ 所诱导的商拓扑)，而这个紧致群的体积(哈测度下)等于 $\sqrt{|D_k|}$，其中的 $D_k$ 是数域 $K$ 的极重要不变量，$K$ 的判别式. $K^*$ 在 $J_k$ 中也有相似关系，不过 $J_k$ 要略加修改，缩小一点成 $J_k^0=\{\prod_{\mathscr{P}\in\mathfrak{S}}\alpha_{\mathscr{P}}\mid\prod_{\mathscr{P}\in\mathfrak{S}}\varphi_{\mathscr{P}}(\alpha_{\mathscr{P}})=1\}$(这里，$\varphi_{\mathscr{P}}$ 都是标准化了的赋值). 于是，$K^*$ 是 $J_k^0$ 的离散子群，$J_k^0/K^*$ 是紧致交换拓扑群，在适当选取局部紧群 $J_k$ 的哈测度(称为塔马伽瓦(Tamagawa)测度)下，$J_k^0/K^*$ 的体积为

$$K=\frac{2^{r_1}(2\pi)^{r_2}hR}{w\sqrt{|D|}},$$

其中 $h$ 为 $K$ 的类数，$R$ 为 $K$ 的控制数，$r_1$ 为与 $K$ 同构的实域数，$r_2$ 为与 $K$ 同构的复域数，$D$ 为 $K$ 的判别式数，$w$ 为 $K$ 中所含单位根数. 这是一个很有用的奇妙的公式.

## 7. 类域论与互反律

类域论是代数数论中最深入的课题之一. 对代数数域 $K$，希望对某一类 $K$ 的扩域用一些群来刻划，如 $L/K$ 是有限正规扩域，那么 $L$ 与 $K$ 之间的所有中间域与 $\mathrm{Gal}(L/K)$ 的子群一一对应，这是伽罗瓦理论. 类域理论希望用 $K^*$ 内部的某些群来刻划，而且还希望这些子群的结构能反映出 $K$ 到 $L$ 之间理想的分解. 希尔

伯特第一个给出了这样的结论：数域 $K$ 的不分歧交换*)扩域全体 $\{L\}$ 与 $K$ 的理想类群 $\mathscr{H}$ 之间有一一对应．与理想类 $I$ 所对应的不分歧交换扩域 $L_I$，就称为 $I$ 的"绝对类域"，现在称为"希尔伯特类域"．$K$ 的任一不分歧交换扩域都是某一理想类的希尔伯特类域．这就是用 $K^*$ 内部的群（理想类群）来刻划 $K$ 的所有不分歧交换扩域．其实，在希尔伯特之前，库默尔的理论也已经表示出这种思想．设 $L/K$ 是有限交换扩张，如果 $\mathrm{Gal}(L/K)$ 的元素的阶的最小公倍数为 $n$，且 $K$ 包含 $n$ 次单位根，则称 $L$ 为 $K$ 的"库默尔 $n$-扩张"，于是，有库默尔定理：在 $K$ 的库默尔 $n$-扩张全体与 $K^*$ 的子群集合 $\{W \mid W \supseteq K^n,\ (W:K^n) < \infty\}$（这里 $K^n$ 是 $K^*$ 中元素的 $n$ 次幂所成的乘法群）之间有一一对应．这种 $W$ 是 $K^*$ 内部的群，用来刻划 $K$ 的库默尔 $n$-扩张．

早在希尔伯特之前，克朗涅克（L. Kronecker）与韦伯（H. Weber）对 $K=\mathbf{Q}$ 的情况证明了一个精彩的定理：对 $\mathbf{Q}$ 的任一有限交换扩域 $F$，总存在正整数 $m$，使得 $F \subseteq \mathbf{Q}(\zeta_m)$，其中 $\zeta_m$ 为 $m$ 次单位根．$\mathbf{Q}$ 上的简单扩域 $\mathbf{Q}(\zeta_m)$ 称为"$m$-次分圆域"．这个定理简单说就是：$\mathbf{Q}$ 上的交换扩域都包含于分圆域之中．满足定理的最小的 $m$，称为交换扩域的导子（*conductor*）．根据这个定理，把所有单位根扩张到 $\mathbf{Q}$ 上，得到一个域 $\mathbf{Q}_{abe}$，它包含所有的有限交换扩域，$\mathbf{Q}_{abe}$ 是最大的交换扩域，不过它是 $\mathbf{Q}$ 的无限扩域．根据导子 $m$ 可以做出 $\mathbf{Q}^*$ 中的某子群 $I_m$ 来．于是 $\mathbf{Q}$ 的所有有限交换扩域的集合与 $\mathbf{Q}^*$ 中子群 $I_m$ 集合一一对应．而且，若 $F$ 与 $I_m$ 对应时，有 $\mathrm{Gal}(F/\mathbf{Q}) \cong \mathrm{Gal}(\mathbf{Q}(\zeta_m)/\mathbf{Q})/I_m$．这就是 $\mathbf{Q}$ 上的类域论，后者是 $\mathbf{Q}$ 上的互反律，就是 $\mathbf{Q}$ 中的某些对象去刻划 $\mathrm{Gal}(F/\mathbf{Q})$．那么，对一般的代数数域 $K$ 怎样？这是 1900 年希尔伯特提出的 23 个问题中的第九问题：数域 $K$ 上的互反律．这个问题于 1927 年由阿

---

*) $L/K$ 称为交换扩域，如果 $L/K$ 是伽罗瓦的，而且 $\mathrm{Gal}(L/K)$ 是交换群．$L/K$ 称为不分歧扩域，如果 $O_K$ 中任一素理想 $\mathscr{P}$ 扩充成 $O_L$ 中理想 $\mathscr{P}O_L$ 时，$\mathscr{P}O_L$ 的分解 $\mathscr{P}O_L=\bar{\mathscr{P}}_1^{e_1}\cdots\bar{\mathscr{P}}_s^{e_s}$，$\bar{\mathscr{P}}_1, \cdots, \bar{\mathscr{P}}_s$ 为不同的 $O_L$ 中素理想，则 $e_i=1$，$i=1, \cdots, s$．

廷解决，给出了一般互反律．希尔伯特第十二问题是问对任何代数数域 $K$ 如何构作 $K$ 的极大交换扩张．这是克朗涅克-韦伯定理(对 $\mathbf{Q}$)的扩充．克朗涅克曾经猜测过，对二次域可以作一个极大交换扩张，他称这个猜想为"青春之梦"．这个问题已经有了一些结果：若 $K$ 为虚二次域，则 $K$ 的极大交换扩域可以由 $K$ 及周期比例为 $K$ 中代数整数 $\tau$ 的椭圆函数的值而生成．至于希尔伯特第十二问题的解决，还相去甚远．

讨论这两个问题都要求有类域理论．1920 年前后，日本数学家高木贞治创建了一般代数数域 $K$ 上的类域理论，他的功绩是：建立了 $K$ 的有限交换扩域 $L$ 的集合与 $K$ 中理想所成乘法群 $I$ 的某些子群 $H$ 所成集合之间的一一对应关系，并且给出了 $\mathrm{Gal}(L/K)$ 与某理想类群之间的同构．后来，阿廷把这个同构更具体有效地写出来，就是一般互反律，它包含著名的高斯(C. F. Gauss, 1777～1855)在数论上的互反律．

1940 年左右，舍瓦莱引进了 idélé 的概念，使得类域理论更容易理解些．先谈谈局部类域论，即局部域上的类域论．设 $K$ 为局部域，$L$ 为 $K$ 的有限交换扩域，$x\in L$ 关于 $K$ 的 norm 记作 $N_{L/K}x$．定义为 $N_{L/K}x=\prod\limits_{\sigma\in\mathrm{Gal}(L/K)}\sigma(x)$，又以

$$N_{L/K}L^*=\{N_{L/K}x\mid x\neq 0,\ x\in L\},$$

这是 $K^*$ 的子群，于是局部类域论的基本定理是：

$$K^*/N_{L/K}L^*\cong\mathrm{Gal}(L/K).$$

这个同构关系就是互反律．这里得出有限交换扩域 $L$ 对应到 $K^*$ 的子群 $N_{L/K}L^*$，这是 $K^*$ 作为拓扑群的一个有限指数的开子群．反之，凡是 $K^*$ 的有限指数的开子群都是这个形式(即存在 $K$ 的有限交换扩域 $L$，使它为 $N_{L/K}L^*$)．因此，$K$ 的有限交换扩域 $L$ 的集合与 $K^*$ 中有限指数的开子群 $N_{L/K}L^*$ 的集合一一对应，而且有伽罗瓦群的同构．这就是局部类域论与互反律．$L$ 称为开子群 $N_{L/K}L^*$ 类域。

如果 $K$ 是整体域，$L$ 是 $K$ 的有限交换扩域，$J_L$、$J_K$ 各为 $L$ 与 $K$ 的 idélé 群．要适当定义从 $J_L$ 到 $J_K$ 的同态 $N_{L/K}: J_L \to J_K$．对 $(z_{\bar{\mathscr{P}}}) \in J_L$，定义 $N_{L/K}(z_{\bar{\mathscr{P}}}) = (x_{\mathscr{P}}) \in J_K$，这里每个 $K$ 的位 $\mathscr{P}$ 上 $x_{\mathscr{P}} = \prod_{\bar{\mathscr{P}}|\mathscr{P}} N_{L\bar{\mathscr{P}}/K\mathscr{P}} z_{\bar{\mathscr{P}}}$，乘积是跑过所有 $\mathscr{P}$ 的因子 $\bar{\mathscr{P}}$，于是对整体域的类域论的基本定理，是存在标准同构

$$J_K/N_{L/K}J_L \cong \mathrm{Gal}(L/K).$$

这是一般互反律．$K$ 的任一有限交换扩域 $L$ 对应 $J_K$ 的有限指数的开子群 $N_{L/K}J_L$；反之，任一 $J_K$ 的有限指数的开子群都是这个形式(存在 $L$)．于是，$K$ 的有限交换扩域 $L$ 的存在与 $J_K$ 的有限指数开子群一一对应．$L$ 称为 $N_{L/K}J_L$ 的类域．

类域都是对交换扩域来分类，而非交换扩域的类域理论与互反律应该是怎样？这是大家所关心的一个课题．

## 8. 序　　域

序域是域的理论中一个重要方向，它与赋值、逻辑等有着密切关系．我们知道，有理数域 $\mathbf{Q}$、实数域 $\mathbf{R}$ 都是有序的，复数域 $\mathbf{C}$ 与二次域 $\mathbf{Q}(i)$ 都不能有序，因为 $i^2=-1$，平方数总该正，$-1$ 总该负，这个数 $i^2=-1$ 又正又负，这就矛盾了．那么，究竟什么叫域有序？序是否可以用代数运算反映出来？同一个域，是否可以有几个序？等等．这就要研究序域．

设域 $K$ 中有一个子集 $P$(称作为非负元素集)，满足：

(i) $P+P \subseteq P$;

(ii) $P \cdot P \subseteq P$;

(iii) $P \cup (-P) = K$;

(iv) $P \cap (-P) = \{0\}$,

于是，$(K, P)$ 就称为**序域**．

很容易得出 $K$ 中平方和都属 $P$，平方和全体记作 $\sigma(K)$，$\sigma(K) \subseteq P$；$-1 \notin P$；$P \neq K$；有限域没有序，$\mathbf{C}$ 没有序等．$\mathbf{Q}$ 与 $\mathbf{R}$

有序而且是唯一序.

是阿廷与斯莱尔(O.Schreier)最先系统地研究序域，于1927年发表了两篇奠基性的文章. 首先一个基本定理是解决怎样的域可以有序. 他们定义：域 $K$ 称为形式实域，如果在 $K$ 中有 $a_1^2+\cdots+a_r^2=0$, $a_i\in K$，则必所有 $a_i=0$, $i=1, \cdots, r$. 这个条件与 $-1\notin\sigma(K)$ 是一样的. 于是，有定理：域 $K$ 可以有序当且仅当 $K$ 是形式实域. 这定理的必要性是显然的；证明充分性时，是先把 $K$ 放到实闭域 $R$ 中去(所谓实闭域，就是这种形式实域，它没真代数扩张的形式实域)，然后实闭域 $R$ 有唯一的序，把这个序局限在 $K$ 上，就得到 $K$ 的序. 包含形式实域 $K$ 的实闭域 $R$ 的存在性，是容易证明的，只要运用佐恩(M. Zorn)引理逐步做出来就可以了. 有意义而且有趣的是，实闭域有而且只有一个序. 实闭域就像实数域 $\mathbf{R}$ 那样. 阿廷证明了实闭域的特性，有定理：

对域 $\mathbf{R}$ 来说，下列三条件是等价的：

(1) $\mathbf{R}$ 是实闭域；

(2) $\sqrt{-1}\notin\mathbf{R}$(即 $x^2+1=0$ 在 $\mathbf{R}$ 中无解，或 $-1$ 不是平方)，而 $\mathbf{R}(\sqrt{-1})$ 是代数闭域；

(3) $\mathbf{R}$ 为形式实域，$|\mathbf{R}^*/\mathbf{R}^{*2}|=2$，且 $\mathbf{R}[x]$ 中任一奇次多项式在 $\mathbf{R}$ 中有根.

显然，实数域 $\mathbf{R}$ 是满足条件(3)的，因此 $\mathbf{R}$ 是实闭域；于是，由(2)就得出 $\mathbf{C}=\mathbf{R}(\sqrt{-1})$ 是代数闭域，这就是高斯所证明的代数基本定理. 实闭域具有实数域 $\mathbf{R}$ 那样的性质，所以，在 $\mathbf{R}$ 上所成立的一些定理(如斯图姆(J.ch. F. Sturm)定理、洛尔(M. Rolle)定理、西尔维斯特(J. J. Sylvester)关于实二次型的惰性定律等)在实闭域上也能成立. 1948年，塔斯基(A. Tarski)运用实闭域给出了数理逻辑中的“塔斯基原理”：设语句(*statement*)$S$ 是用序域的初等语言来表达的，则 $S$ 在某实闭域中成立当且仅当 $S$ 在所有实闭域中成立，实闭域的理论对非标准分析理论也有应用.

阿廷于1927年，运用形式实域的理论，解决了著名的希尔伯

特第十七问题，这就是定理：

设 $F$ 是实数域 $\mathbf{R}$ 的子域，它有唯一序，又 $f\in F(x_1, \cdots, x_n)$ 为 $n$ 个变量 $x_1, \cdots, x_n$ 的有理函数，而且 $f$ 半正定，即 $f(a_1,\cdots,a_n)\geqslant 0$ 对所有 $a_i\in F$（只要在 $f$ 的定义区内）．则 $f$ 是域 $F(x_1,\cdots,x_n)$ 中的一个平方和（即 $f=g_1^2+\cdots+g_r^2$, $g_i\in F(x_1, \cdots, x_n)$）．

阿廷的理论没有说明 $f$ 表成平方和时需要多少个平方项，但是希尔伯特早在 1893 年就知道，任意两个变量（$n=2$）的半正定有理函数是四个平方和（$r=4$）．1966 年，阿克丝（J. B. Ax）指出，三个变量（$n=3$）的半正定有理函数是八个平方和（$r=8$）；并且，猜测 $n$ 个变量的半正定有理函数是 $2^n$ 个平方和．1967 年，普费斯特（A. Pfister）证明了这个猜测．用了非常巧妙的方法，从而也大大推动了二次型的理论的进展．

实域的理论很丰富，已经成为代数中的一个分支．